

Enclosure to:  
JWS-04-003

**JWR-04-001**  
**JBD01**

# **Wireless Networks Summit**

**January 2004**





**JWR-04-001**  
**JBD01**

# Wireless Networks Summit

**JOINT WAREFARE ANALYSIS DEPARTMENT**

THE JOHNS HOPKINS UNIVERSITY • APPLIED PHYSICS LABORATORY

Johns Hopkins Road, Laurel, Maryland 20723-6099



## *Table of Contents*

<b>LIST OF FIGURES .....</b>	<b>iii</b>
<b>EXECUTIVE SUMMARY .....</b>	<b>v</b>
<b>I. INTRODUCTION.....</b>	<b>1</b>
1.1 Purpose .....	1
1.2 Summit Objectives .....	1
1.3 Background .....	2
1.4 Summit Agenda and Methodology .....	2
1.5 Summit Participants .....	3
<b>II. OBSERVATIONS.....</b>	<b>5</b>
2.1 Information Assurance and Policy Were the Dominant Topics.....	5
2.2 Need Documented Requirements.....	6
2.3 Wireless Networks Applications.....	7
2.4 Wireless Mission Capabilities.....	7
2.5 Opportunities for Test and Evaluation .....	8
2.6 Community of Interest .....	9
2.7 Industry Day.....	9
2.8 Roadmapping .....	9
2.9 Additional Observations.....	10
<b>III. CONCLUSION .....</b>	<b>11</b>
<b>APPENDIX A: AGENDA .....</b>	<b>A-1</b>
<b>APPENDIX B: SUMMARY BRIEFING.....</b>	<b>B-1</b>
<b>APPENDIX E: INTRODUCTORY SURVEY RESULTS.....</b>	<b>E-1</b>
<b>APPENDIX F: DAY ONE SURVEY RESULTS .....</b>	<b>F-1</b>
<b>APPENDIX G: SUMMARY SURVEY RESULTS .....</b>	<b>G-1</b>
<b>APPENDIX H: GROUPWARE COMMENTS.....</b>	<b>H-1</b>
<b>APPENDIX I: REFERENCES .....</b>	<b>I-1</b>

Intentionally Left Blank

**LIST OF FIGURES**

Figure 1: Agenda..... 2

Figure 2: Summit Participants ..... 4

Intentionally Left Blank



## EXECUTIVE SUMMARY

The Naval Network Warfare Command (NETWARCOM) and Program Executive Office (PEO) Ships sponsored the Wireless Networks Summit held at The Johns Hopkins University Applied Physics Laboratory (JHU/APL) on 8-10 December 2003.

The Wireless Networks Summit was designed to gather a community of interest (COI) to address naval wireless technologies. This first meeting of the wireless networks COI was to identify group members, initiate a dialog and lay the foundation for subsequent efforts. The summit objectives were to:

- Assemble stakeholders for information exchange
- Establish a community of interest for naval wireless networks
- Identify wireless issues in the areas of information assurance, technical, policy, and operational requirements, implementation and acquisition
- Identify potential wireless applications
- Identify mission capabilities
- Identify opportunities for test and evaluation
- Develop a common approach (roadmap) for the rapid and efficient delivery of wireless networking capabilities to the warfighter

The Wireless Networks Summit was conducted over a three-day period, 8-10 December 2003, with two days designated for topic of interest presentations and discussions and one day for Industry Day. The first day began with opening remarks by CAPT Kevin Uhrich of NETWARCOM and Mr. Glen Sturtevant of PEO Ships. Opening remarks were followed by an overview of wireless networks and issues discussion by members of the SmartShip program and Space & Naval Warfare Systems Command (SPAWAR). The remainder of the day consisted of the presentation of four case studies and discussions. Industry Day was held on the second day. It was a combination of vendor demonstrations and presentations along with three plenary sessions. The third day continued with topic of interest presentations and discussions from the first day. Morning sessions presented naval wireless applications and capabilities, technology insertion, and opportunities for test and evaluation to stimulate discussions in these focus areas. The summit closed with a roadmap methodology description and a presentation of the way ahead.

A total of 76 people attended the summit. The majority of the participants had technical backgrounds in areas of engineering and communications.

Wireless network security and policy were the dominate issues expressed during the summit. The leading cause of these issues was an absence of a clear and approved Navy policy governing wireless networks. The result has been a slow and challenging deployment of commercial wireless equipment into the fleet. Currently, there are several wireless network policies and standards waiting approval which are anticipated to relieve most of the problems. The Department of Defense (DoD) Directive 8100.bb "*Use of Commercial Wireless Devices*,

*Services, and Technologies in the DoD Global Information Grid*” along with several Navy specific policies and standards developed to support 8100.bb will set the framework for future wireless network implementation into the fleet.

Several participants expressed concern that the cost savings of commercial off-the-shelf (COTS) products could be lost due to stringent security standards and policy. Commercial vendors have tended to limit security features in favor of ease of configuration, implementation and lower cost. The rapid turn-over of COTS was also cited as a concern and may limit life-cycle savings. A clear business case which demonstrates benefits such as cost savings, improved productivity, and process improvement within defined and stated metrics is critical for full consideration of wireless technology.

Opportunities for test and evaluation of wireless networks have been difficult due to the absence of consistent procedures and standards and operational demands on ships. Participants stated clearly that there needs to be an emphasis upon shipboard testing under actual conditions of use. Previous test and evaluation efforts have emphasized computer networking using the 802.11b wireless standard. Future test and evaluation activities should be expanded to address other wireless applications and standards. Remote data application and remote monitoring and control were of particular interest to the participants.

Overall, the Wireless Networks Summit was a productive exchange of information, issues, and perspectives that will benefit future wireless technology development, test and evaluation, implementation, and acquisition. The participants were positive about their summit experience and felt that the event had met all its objectives.

## I. INTRODUCTION

### 1.1 PURPOSE

The purpose of this report is to summarize the Wireless Networks Summit sponsored by the Naval Network Warfare Command (NETWARCOM) and Program Executive Office (PEO) Ships SmartShip program and conducted at The Johns Hopkins University Applied Physics Laboratory (JHU/APL) on 8-10 December 2003. This document provides a brief description of the summit and the observations of the JHU/APL analysis team.<sup>1</sup> Detailed information, including a summit Summary Briefing, is contained in the appendices to this report.

### 1.2 SUMMIT OBJECTIVES

The objectives of the Wireless Networks Summit were to:

- Assemble stakeholders for information exchange
- Establish a community of interest for naval wireless networks
- Identify wireless issues in the areas of information assurance, technical, policy, and operational requirements, implementation and acquisition
- Identify potential wireless applications
- Identify mission capabilities
- Identify opportunities for test and evaluation
- Develop a common approach (roadmap) for the rapid and efficient delivery of wireless networking capabilities to the warfighter

### 1.3 BACKGROUND

The Navy's SmartShip program has identified wireless networks as a key technology to increase current capabilities and reduce shipboard manning requirements with the goal of reducing overall cost. However, the inclusion of commercial wireless networks and standards into the Navy has created technical policy and requirements issues in the areas of information assurance, test and evaluation, and safety. With no consistent policy and requirement standards and procedures in place, a wireless moratorium message was issued 192206Z AUG 03 titled "Cessation of WLAN Installations in COMPACFLT and COMLANFLT Ships" which stopped all implementation of wireless networks on Navy ships. The only exception to this moratorium was the USNS *Coronado* and USS *Mason* which were conducting pre-existing wireless local area network (WLAN) testing and evaluation.

The Wireless Networks Summit was the first opportunity to gather a community of interest (COI) to address wireless issues. The COI was given a vision, "to create and foster an innovative environment to harness the transformational potential of wireless network

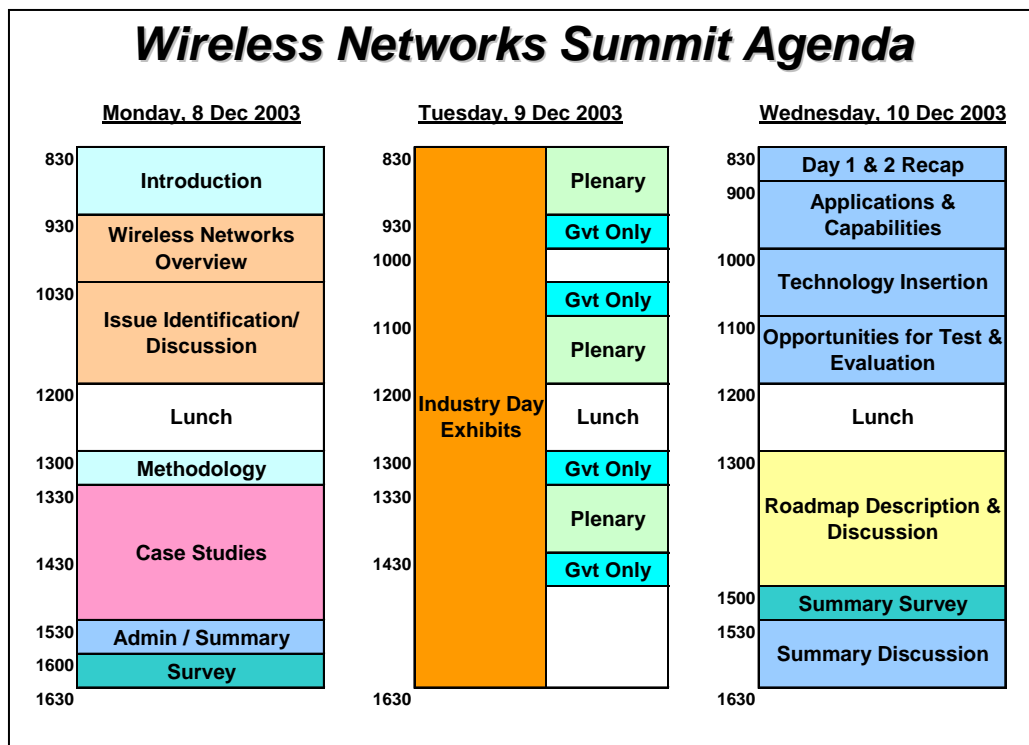
---

<sup>1</sup> The JHU/APL seminar team consisted of A. G. Arnold, H. W. Kim and J. M. Nolen.

technologies for the US Navy,” and a mission, “to align and leverage resources and opportunities through a collaborative process to enable wireless network technologies throughout the Navy’s operational and business operations.”<sup>2</sup>

## 1.4 SUMMIT AGENDA AND METHODOLOGY

The Wireless Networks Summit was conducted over a three-day period, 8-10 December 2003. Figure 1 illustrates the summit agenda. Day One began with opening remarks by the Naval Networks (N6) Division Director, CAPT Kevin Uhrich, and PEO Ships SmartShip Program Manager, Mr. Glen Sturtevant. These remarks were followed by a wireless networks overview, issue identification and discussion presented by the SmartShip Wireless Integrated Planning Team (IPT) Lead, Mr. David Bartlett, and Space & Naval Warfare Systems Command (SPAWAR) representatives. CDR Larry Pemberton presented an overview of the DoD Directive 8100.bb. The remainder of the first day consisted of case studies that presented results and lessons learned on WLAN installation and sea trials on board four different surface platforms.



**Figure 1: Agenda**

Day Two (9 December 2003) was designated Industry Day and held in the Kossiakoff Center, a conference facility on the JHU/APL campus. The purpose of Industry Day was to provide a forum for vendors with wireless products to demonstrate or discuss their products with key Navy decision makers involved with wireless technology. Several of the vendors held

<sup>2</sup> Wireless Networks Summit Opening Presentation by SmartShip Wireless IPT Lead, Mr. David Bartlett.

“Government Only” sessions in order to share proprietary information with government attendees. There were three plenary sessions also held during the day; they covered an overview of the Department of Defense (DoD) Global Information Grid (GIG), a summary of DoD and Navy requirements and policy, and FORCENet.

The last day of the summit provided an opportunity to present and discuss key topics of interest dealing with wireless applications and capabilities, technology insertion, and opportunities for test and evaluation. A presentation of a roadmapping methodology along with preliminary roadmap results was presented and discussed. The summit ended with a summary discussion of “The Way Ahead” which detailed the steps and requirements for moving forward to continue the COI efforts started and momentum gained during this summit.

Appendix A provides a more detailed agenda. Appendix B contains the summit Summary Briefing, which describes the agenda and methodology for this summit.

The Wireless Networks Summit employed groupware, a network of laptop computers equipped with collaboration software that enabled the participants to record comments and to respond to other participants’ comments throughout the summit.

## **1.5 SUMMIT PARTICIPANTS**

The summit involved a total of 76 participants, although not all participants were present for the entire three days. The following list describes the 76 attendees by general categories:

- |                  |                 |
|------------------|-----------------|
| • 6 NETWARCOM    | • 1 OPNAV       |
| • 5 SmartShip    | • 16 Other Navy |
| • 9 Other NAVSEA | • 3 USMC        |
| • 9 SPAWAR       | • 1 JFCOM       |
| • 6 Fleet        | • 1 NSA         |
| • 2 NAVAIR       | • 8 Contractor  |
| • 4 ONR          | • 5 Other       |

Figure 2 is a photograph of the summit participants taken on the morning of Day One (8 December 2003). Appendix C is the list of summit participants. Appendix D is the original invitation issued by the Navy NETWARCOM and PEO SHIPS SmartShip summit planning team.



**Figure 2: Summit Participants**

## II. OBSERVATIONS

The Wireless Networks Summit Summary Briefing prepared by the JHU/APL team is provided in Appendix B and describes the summit agenda, methodology, groupware results, numerical results of the introductory, Day One and summary surveys, and the JHU/APL observations. The detailed results of the surveys are listed in Appendices E, F and G. Appendix H contains the groupware comments collected during the summit. Appendix I is a list of references used to design and conduct the seminar.

The following paragraphs summarize the major JHU/APL observations. These observations represent a synthesis of the verbal discussion, the comments entered into groupware, and the participants' responses to the summit survey questions.

### 2.1 INFORMATION ASSURANCE AND POLICY WERE THE DOMINANT TOPICS

During the summit, information assurance and policy issues were the dominant topics of discussion related to wireless networks. Information assurance and policy as they pertain to network security were the focus of several summit presentations including the case studies. Security policies and security standards were also the two most common areas of contention among the summit participants and took up the majority of the group discussions, both verbal and those in groupware. Significant opinions expressed include:

- There is an incomplete set of clear, approved wireless security standards and policy for wireless networks to effectively implement them onboard ships.
- Security measures have far exceeded the level of vulnerability or the threat and makes implementation of wireless networks impractical and too costly.
- Not enough is known about possible vulnerabilities and the risk of security breeches must be minimized.

#### 2.1.1 Absence of Clear, Approved Policies May be a Greater Obstacle Than Stringent In-Place Policies

For wireless networks, the acquisition and implementation process without a clear, approved policy has been a greater obstacle than if stringent policies were in place. For the Navy this manifestation resulted in the halt of all wireless network installation in both the Pacific and Atlantic fleets with a moratorium message issued on 192206Z AUG 03 titled "Cessation of WLAN installation in COMPACFLT and COMLANFLT ships."

There are several policies expected to be approved soon which should resolve most of the obstacles to implementing wireless networks. One highly anticipated policy, DoD Directive 8100.bb "*Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid*," was presented by CDR Larry Pemberton during the wireless networks overview. In addition, NETWARCOM intends to release a Navy wireless policy which will officially endorse the PMW 165 Wireless LAN Technical Guidance document. The document

will provide a compliance matrix with interoperability, security, and environmental requirements along with wireless component specifications.

For many of the summit participants, the issues with information assurance were understood as temporary near-term obstacles that will eventually be resolved with improved implementation, new security standards, and better understanding of the technology and vulnerabilities.

### **2.1.2 Requirements to Meet Navy's Security Standards Threatens the Use of COTS**

There were several points of view concerning the implementation of information assurance standards and policy on wireless networks. There was a consensus that sufficient technology exists to meet the security requirements and policy; however, there was considerable debate on how to implement them. Some of the participants expressed frustration that the current security requirements place significant barriers to implementing any type of wireless networks. Another area of discussion revolved around the classification of data between unclassified, sensitive but unclassified (SBU), and classified. There does not seem to be a uniform policy between the different commands and organizations to deal with the SBU classification; for example Pacific Command (PACOM) requires SBU data be handled the same as classified data for wireless networks. Also, the need to protect the information gained from a collection of unclassified or SBU data, usually at a higher classification level, requires most wireless networks carrying unclassified data to be classified.

Currently, the only approved classified wireless network requires National Security Agency (NSA) Type I certification. It uses a non-commercial standard to encrypt both the data and the packet overhead to mask network activity. Using NSA Type I level security, especially for unclassified networks, creates significant overhead cost and complexity commonly associated with classified networks. Using NSA Type I requires periodic re-keying (usually every 30 to 90 days) and keeping the network access points and network cards in approved classified areas or in secure lock boxes.

Several participants expressed concern that applying excessive security requirements to unclassified networks threatens the use of COTS equipment and many of the benefits associated with wireless networks. As an example, Harris SecNET-11 network card, which features NSA Type I security certification over 802.11b, costs approximately \$2,500. A similar 802.11b network card without such security features costs approximately \$100. In general, industry has been slow to adopt some of the special security requirements for the DoD and Navy due to the cost and complexity involved.

## **2.2 NEED DOCUMENTED REQUIREMENTS**

Documented requirements for wireless networks are necessary in order to support the business case for their use. The business case must detail benefits in terms of cost savings, improved productivity and mission enhancements. These benefits need to be articulated and documented in performance or cost metrics which can be used to justify funding. Several



participants and presenters voiced the need for a wireless champion to push wireless technology into the fleet. An organization or program to take on this role would provide much needed focus and consistency among the Navy wireless network community.

One program of record for wireless networks was acknowledged. The submarine fleet has received approval and funding to install unclassified WLANs in its submarines. The submarine has some unique advantages to minimize unwanted RF emissions but it does have to comply with many of the same safety requirements as any other Navy vessel. There might be some opportunities to leverage lessons learned from this particular program.

## **2.3 WIRELESS NETWORKS APPLICATIONS**

Two basic approaches were expressed on the focus of applications and technology development. Participants were divided between: 1) the need to develop a robust network that can host to-be-developed applications such as those required for the SmartShip program, and 2) the development of a “killer” application that will generate a need for a wireless network capability. Overall, the participants saw the importance of both approaches. The development of applications cannot deliver value without robust networks and user demand, and business cases will drive useful applications.

### **2.3.1 Computer Networking Was Seen as the Most Important Application**

Wireless computer networking was seen as the most important wireless application followed by remote data application and remote monitoring and control.<sup>3</sup> Initially, the 802.11 standards were used primarily for computer networking, but have recently enjoyed considerable growth and interest with remote data applications such as personal digital assistants (PDAs). There was strong interest among the participants towards the use of PDAs and wireless networks to increase productivity and reduce overall cost.

## **2.4 WIRELESS MISSION CAPABILITIES**

Most of the participants felt that mission capabilities are highly dependent upon specific applications and user needs. From survey respondents, security was rated the most important capability<sup>4</sup> and reflects the overall concern over security and policy during the summit. However, the mobility aspect of wireless, which provides convenience of use and was identified as a key benefit by the participants, was probably the single most important capability that distinguished wireless networks over wired.

The other mission capabilities presented were operational range, portability, ease and speed of installation, throughput, and ruggedness. Participants suggested additional capabilities such as interoperability, local computer processor capacity, compatibility with other systems, and

---

<sup>3</sup> Day One Survey Question 9 (Appendix F).

<sup>4</sup> Day One Survey Question 11 (Appendix F).

supportability. Interoperability between Navy and Marine Corps systems was highlighted as a critical capability by the participants. Navy wireless networks on board ships need to allow seamless integration of Marine wireless systems as they board and off-load during military operations.

## **2.5 OPPORTUNITIES FOR TEST AND EVALUATION**

From summit participants' responses and the case study presentations, the absence of documented test requirements and a defined test process have hampered the test and evaluation opportunities for wireless networks. Also, participants cited that past test and evaluation efforts with wireless networks were often conducted independently of each organization resulting in much duplication of effort. They were conducted without well defined technical requirements and test objectives which made the process both lengthy and costly. Better communication and coordination for future events was recommended among the various organizations in the Navy as well as with the Marine Corps.

### **2.5.1 Emphasis Upon Shipboard Testing Under Actual Conditions of Use**

Discussion concerning possible venues for future test and evaluation revealed that emphasis upon shipboard testing under actual conditions of use was the most important. Testing under scheduled ship deployments, sea trials and training exercises were the highest ranked opportunities.<sup>5</sup> The participants indicated the importance of identifying user needs and gaining user acceptance under these stressful conditions. However, there was also recognition of the difficulty with scheduling and operational challenges involved with shipboard testing.

### **2.5.2 Obstacles to Test and Evaluation**

Current obstacles to test and evaluation were divided between two main issues: 1) a lack of common test and evaluation objectives and measures, and 2) operational constraints due to other demands on test organizations, units, and ships.

### **2.5.3 Future Test Opportunities**

A Marine civilian representative shared some WLAN test capabilities of the Marine Corps Tactical Systems Support Activity (MCTSSA) at Camp Pendleton, CA, and offered to collaborate with upcoming Navy efforts. There was also discussion involving the USNS *Coronado* as a dedicated test site for wireless testing since availability of other naval platforms appeared to be very limited due to operational constraints.

---

<sup>5</sup> Day One Survey Question 15 (Appendix F).

## **2.6 COMMUNITY OF INTEREST**

One of the objectives of the summit was to create a COI for wireless networks. The principle efforts identified for the COI were in the area of information sharing and coordination of activities for future events. Some participants identified the need for strict enforcement of policies and standards by the COI, but survey results did not strongly support this.<sup>6</sup> The participants wanted meetings, conferences, websites, and newsletters to be the primary products of the COI, followed by support for proposing policies and standards. Most participants wanted to continue wireless COI activities. Recommendations for future summits included:

1) opportunities to develop actual products to take away from the summit such as policy recommendations, 2) creating subgroups for areas of interest and allowing opportunities to discuss and resolve issues in a smaller setting, and 3) a broader audience with more users and higher level decision makers.

## **2.7 INDUSTRY DAY**

The Industry Day event which was conducted on the second day (9 December 2003) provided 30 vendors the opportunity to market their products and services in a trade-show environment. A factor that probably contributed to the overall interest of Industry Day was the high technology-refresh nature of wireless technology and the opportunity for participants to see certain new products and services for the first time.

Suggestions for improvement for future events included: 1) more displays and presentations, 2) more participation by larger companies such as Motorola and Nextel, and 3) more time for vendor presentations.

## **2.8 ROADMAPPING**

The Roadmapping methodology as presented during the summit for the Naval wireless network was well received. Due to a series of problems with the survey tool program, time constraints, and low survey participation, a meaningful roadmap could not be developed and presentation of the results was limited. The participants were able to review the process and methodology for collecting and organizing the data for future roadmapping exercises. With good survey participation and proper questionnaires, roadmapping could provide a great deal of insight into planning and allocation of resources.

---

<sup>6</sup> Day One Survey Questions 25 and 26 (Appendix F).

## **2.9 ADDITIONAL OBSERVATIONS / OTHER ISSUES DISCUSSED**

### **2.9.1 Summit Focused Primarily on 802.11 Standards**

Much of the summit presentations and case studies dealt with issues and implementation associated with the 802.11 standards and in particular 802.11b. This approach focused discussions around wireless computer networking and limited discussions in other areas such as Radio Frequency Identification (RFID) and remote monitoring and control. Wireless standard 802.11b seems to be the most often used standard and appears to be the de facto Navy standard for wireless networks. The biggest problem with the current 802.11 standards is a lack of a built-in security feature that supports DoD's security requirements. The release of 802.11i is expected to resolve some of these requirements and reduce the cost of implementation.

### **2.9.2 Threats to Wireless Networks**

During discussions concerning security, the participants were unaware of the actual threats to wireless networks and expressed great interest in learning more about potential threats. Since the summit was held at the unclassified level, discussion on this subject was very limited. It is recommended that future summits or events allow opportunities to exchange information concerning actual threats to wireless networks.

### **2.9.3 Extent of Vulnerability and Safety is Not Well Known**

Because wireless networks are a relatively new technology with few documented test cases from the Navy, summit participants expressed uncertainties about the vulnerabilities and safety hazards created by wireless networks in a shipboard environment. These uncertainties appear to have limited the enthusiasm among some summit attendees for wireless networks. One participant asked: "What is the probability of RF emission outside the ship and can it reveal ship position?" Responding to this question and others like it, with authoritative, scientifically-based assessments is a key challenge for the wireless COI.

The safety hazards created by wireless devices, especially high power access points have not been well defined and documented. The certification process associated with Hazards of Electromagnetic Radiation to Fuel (HERF), to Ordnance (HERO), and to Personnel (HERP) was not well understood among the summit participants.

### III. CONCLUSION

The Wireless Networks Summit accomplished its main objectives. It assembled a diverse group from the Navy's wireless community and established a COI. The summit provided opportunities to discuss and identify wireless issues, potential wireless applications and mission capabilities, and opportunities for test and evaluation. It presented a common approach (roadmap) for a rapid and efficient delivery of wireless networking capabilities.

The summit provided an open environment for the active exchange of issues, concerns, and ideas among the diverse group of participants. The presentations provided opportunities to discuss wireless issues and solutions. The case studies detailed lessons learned from previous test and evaluation efforts. Industry Day gave the participants the opportunity to meet industry vendors and ascertain the availability and capability of wireless products and services. The roadmapping presentation focused attention on technology insertion opportunities and the need to coordinate resources among the Navy wireless community to promote the integration of wireless technology into the Fleet.

Wireless network security and policy were the dominant issues discussed during the summit. They were also the main areas of contention among the summit participants. Some participants involved with acquisition and implementation often felt that current security requirements and policies tended to be overly restrictive, and thereby, undermine the use of COTS and user acceptance for wireless networks. In general, users of wireless networks felt that securing the network was the most important factor until more is known about vulnerabilities and other issues associated with wireless technologies.

Summit participants perceived security and policy restrictions as the primary obstacles to implementing wireless networks. However, there was consensus among participants that these issues will be resolved in the near future as technology matures and new and improved security standards and policies are developed and approved.

Interest in the COI for wireless networks was strong among the participants. The SmartShip program made a presentation for the way ahead to bring attention to future COI activities. The way ahead provided much needed structure and purpose. It outlined a course of action and proposed first year deliverables for the COI. During the summit, there were many requests for a Navy wireless champion, but until a program or organization takes on this role, the COI could be viewed as a possible body to facilitate and advocate implementation of wireless technology to the Fleet.

Due to the success of this initial gathering of the Navy's wireless networks community and the interest to continue many of the efforts started during this summit, a follow-up summit is highly recommended.

Overall, the Wireless Networks Summit was a productive exchange of information, issues, and perspectives that will benefit the Navy's wireless community. The participants were positive about their summit experience and felt that the event had met all its objectives.

Intentionally Left Blank

## **APPENDIX A: AGENDA**

### Wireless Networks Summit

8-10 December 2003

Warfare Analysis Laboratory  
The Johns Hopkins University Applied Physics Laboratory

#### **8 December 2003 (Monday)**

Check-in	0800
Introductory Remarks	0830
WAL and GroupWare Orientation	0845
Wireless Networks Overview	0930
Issue Identification and Discussion	1030
Requirements Definition and Discussion	1115
Lunch	1200
Methodology	1300
Case Study 1: SmartShip Wireless	1330
Case Study 2: USS GW WLAN	1400
Case Study 3: USNS Coronado	1430
Case Study 4: USS Elrod	1500
Summary	1530
Day 1 Survey	1600
Adjourn	1630

#### **9 December 2003 (Tuesday)**

Check-in	0800
Industry Day – Kossiakoff Center	0830
Adjourn	1630

#### **10 December 2003 (Wednesday)**

Check-in	0800
Day One/Two Summary	0830
Applications and Capabilities	0900
Opportunities for T&E	1000
Technology Insertion	1100
Lunch	1200
Roadmap Description and Discussion	1300
Summary Survey	1500
Summary Discussion	1530
Adjourn	1600

## Appendix A, Agenda

Intentionally Left Blank



## APPENDIX B: SUMMARY BRIEFING

### TABLE OF FIGURES

Figure 1: Wireless Networks Summit 8-10 December 2003, Summary Briefing .....	3
Figure 2: Agenda.....	3
Figure 3: Event Objectives.....	4
Figure 4: Wireless Networks Summit Agenda, 8-10 December 2003.....	4
Figure 5: Wireless Networks Summit Agenda, 8-10 December 2003.....	5
Figure 6: Wireless Networks Summit 76 Participants.....	5
Figure 7: Day One, 8 December 2003 .....	6
Figure 8: Industry Day, 9 December 2003.....	6
Figure 9: Day Three, 10 December 2003.....	7
Figure 10: GroupWare Results: 925 Comments (368 Main, 557 Referring) .....	7
Figure 11: Opinion Surveys .....	8
Figure 12: Experience .....	8
Figure 13: Description .....	9
Figure 14: Expectations .....	9
Figure 15: Benefits of Wireless Networks.....	10
Figure 16: Wireless Network Uses in 2005 .....	10
Figure 17: Wireless Network Users in 2010.....	11
Figure 18: Obstacles to Implementing Wireless Networks .....	11
Figure 19: Challenges to Delivering Wireless Networks .....	12
Figure 20: Key Lessons of Case Studies.....	12
Figure 21: Wireless Applications.....	13
Figure 22: Wireless Capabilities.....	13
Figure 23: Test and Evaluation Venues .....	14
Figure 24: Test and Evaluation Measures.....	14
Figure 25: Test and Evaluation Obstacles .....	15
Figure 26: Role of COI .....	15
Figure 27: Priority of Effort.....	16
Figure 28: Potential Products.....	16
Figure 29: Priority of Issues.....	17
Figure 30: Day One Assessment.....	17
Figure 31: Industry Day Assessment .....	18
Figure 32: Roadmapping Assessment.....	18
Figure 33: Expectations and Overall Assessment.....	19
Figure 34: Recommendation for Future Wireless Activities .....	19
Figure 35: Future Attendance .....	20
Figure 36: APL Observations (1 of 11) Security and Policy .....	20
Figure 37: APL Observations (2 of 11) Need Documented Requirements .....	21
Figure 38: APL Observations (3 of 11) Wireless Networks Applications .....	21
Figure 39: APL Observations (4 of 11) Wireless Networks Capabilities.....	22
Figure 40: APL Observations (5 of 11) Opportunities for Test and Evaluation.....	22
Figure 41: APL Observations (6 of 11) Community of Interest (COI) .....	23
Figure 42: APL Observations (7 of 11) Industry Day .....	23

## Appendix B, Summary Briefing

Figure 43: APL Observations (8 of 11) Roadmapping.....	24
Figure 44: APL Observations (9 of 11) Additional Points .....	24
Figure 45: APL Observations (10 of 11) Additional Points (cont.).....	25
Figure 46: APL Observations (11 of 11) Summit Design and Administration .....	25
Figure 47: Summary .....	26

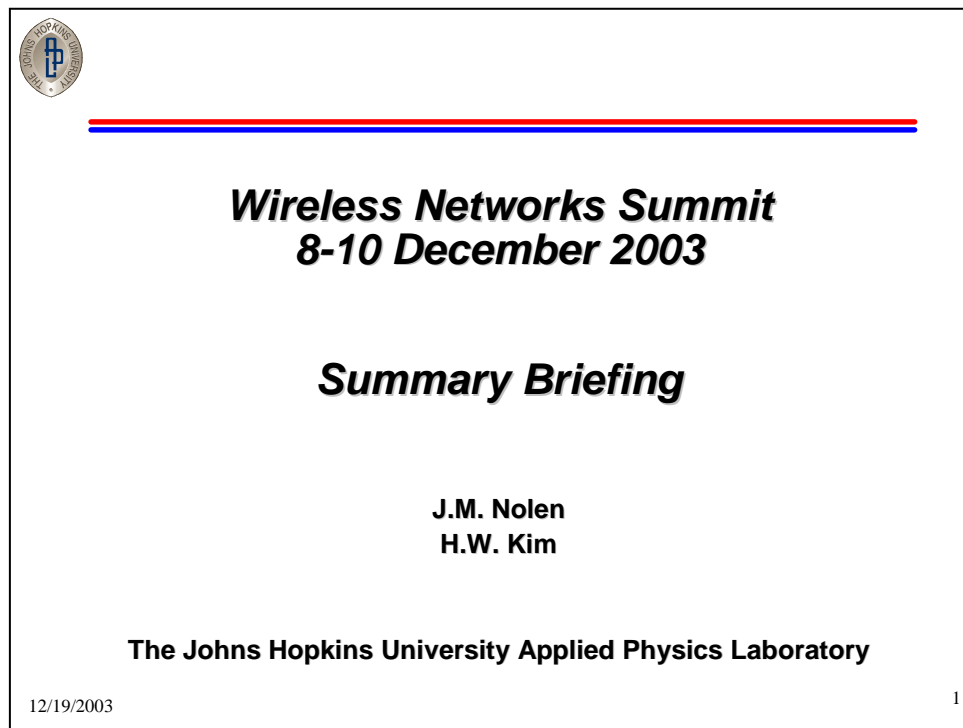


Figure 1: Wireless Networks Summit  
8-10 December 2003

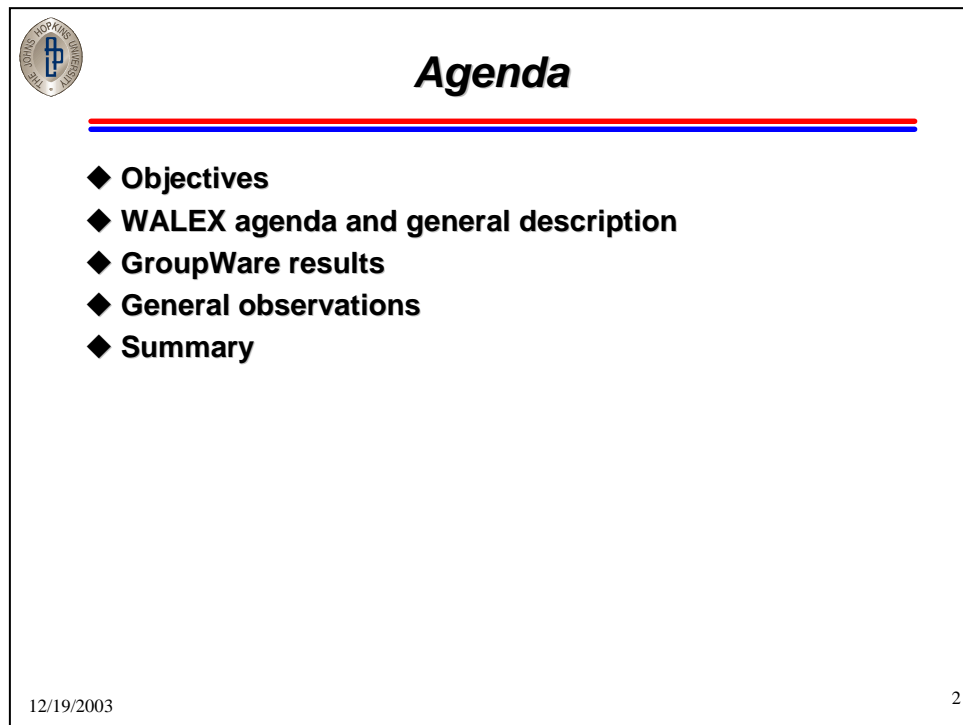


Figure 2: Agenda

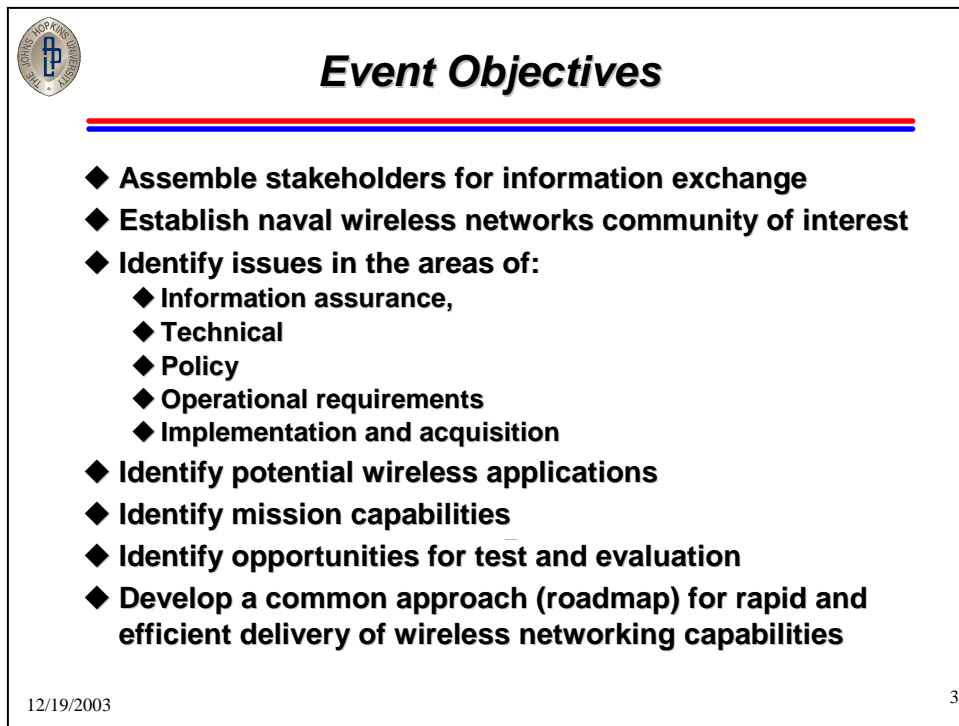


Figure 3: Event Objectives

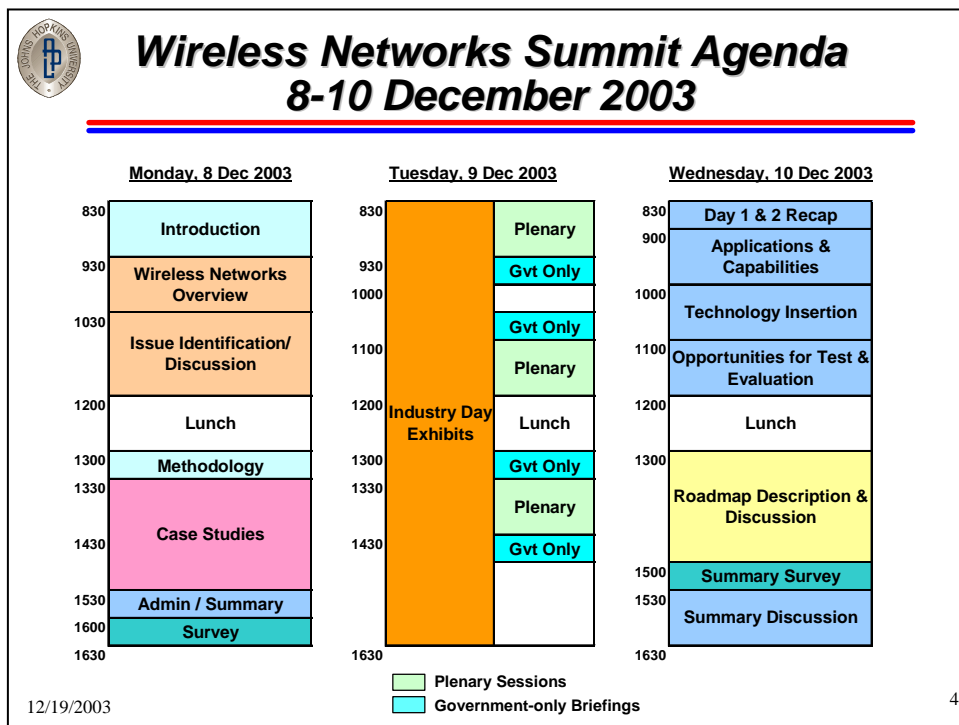


Figure 4: Wireless Networks Summit Agenda  
8-10 December 2003

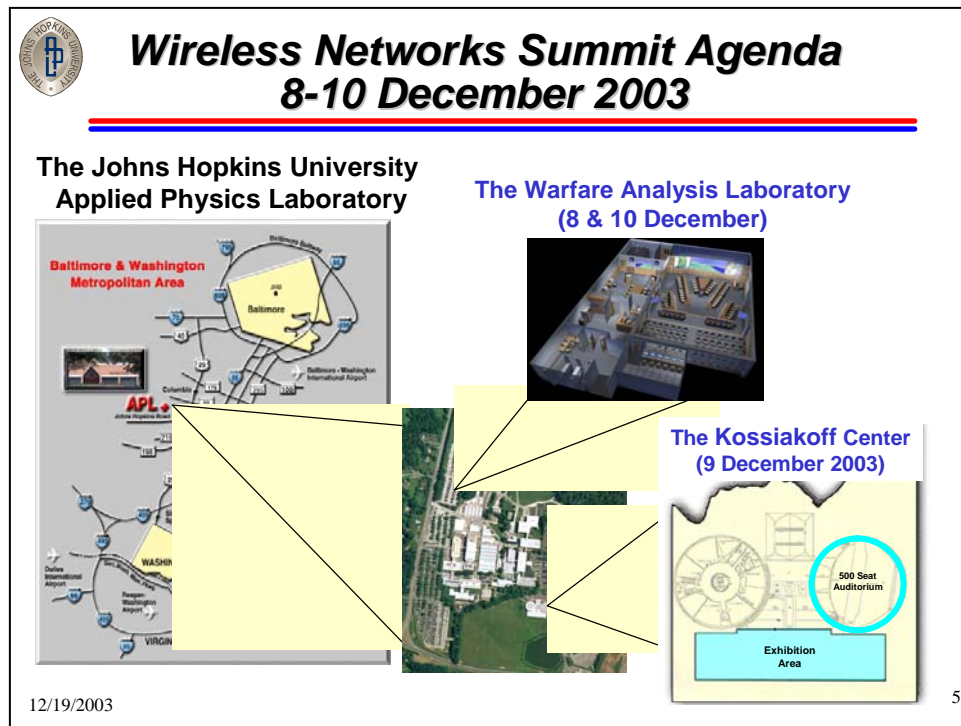


Figure 5: Wireless Networks Summit Agenda  
8-10 December 2003

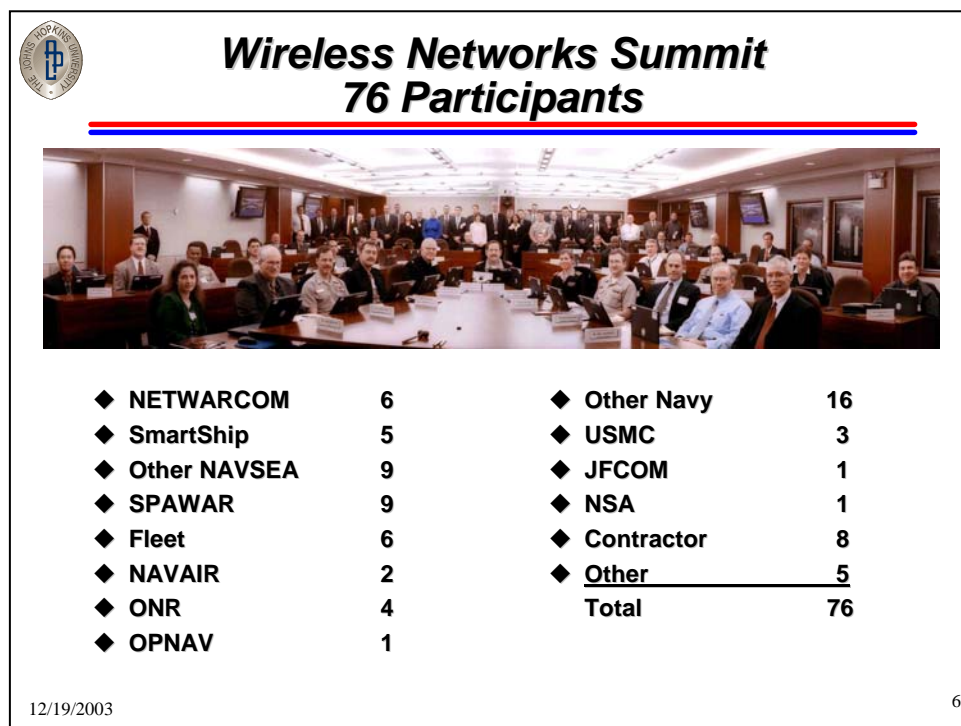


Figure 6: Wireless Networks Summit  
76 Participants

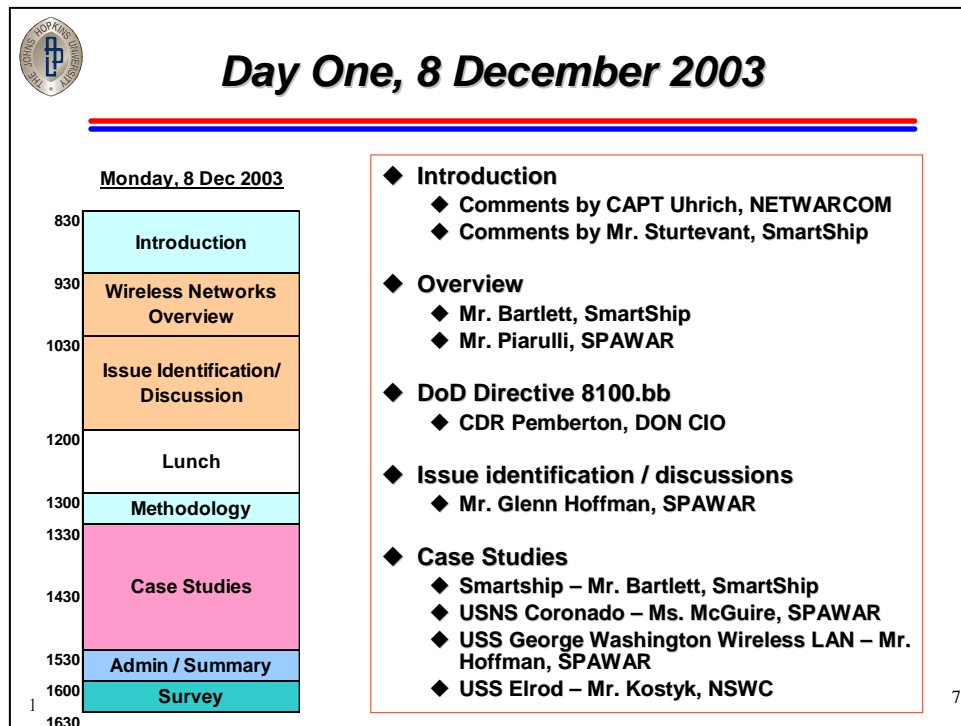


Figure 7: Day One, 8 December 2003

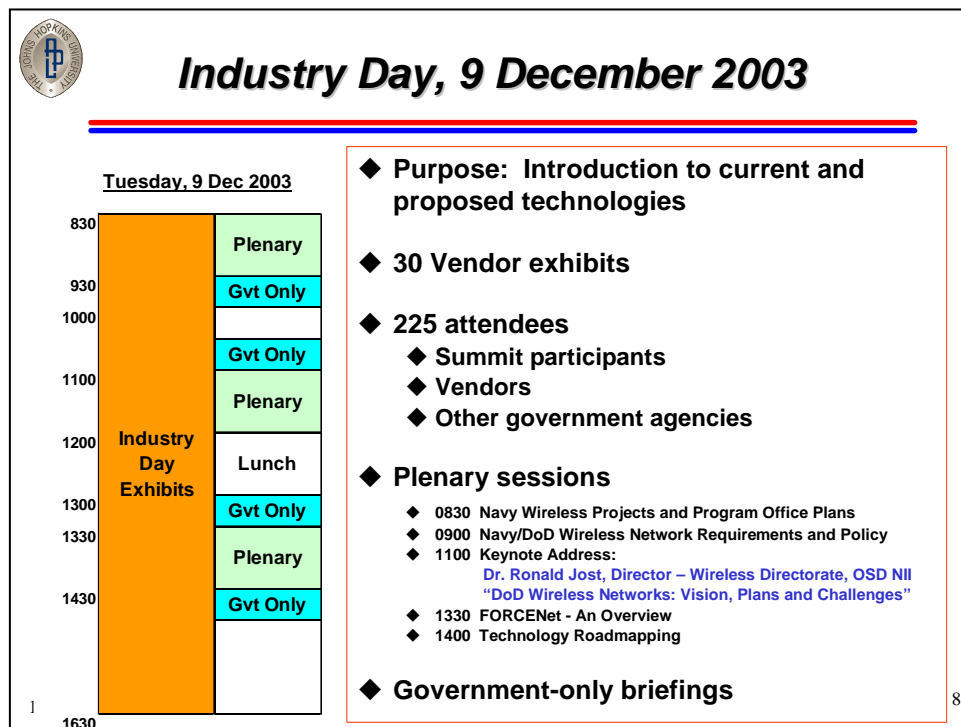


Figure 8: Industry Day, 9 December 2003

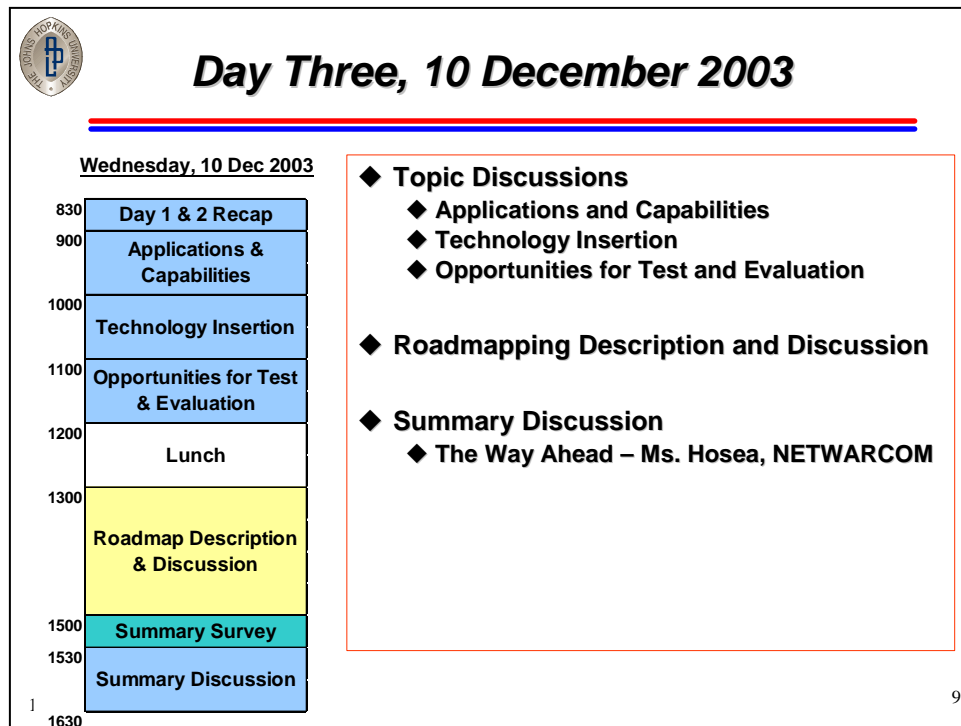


Figure 9: Day Three, 10 December 2003

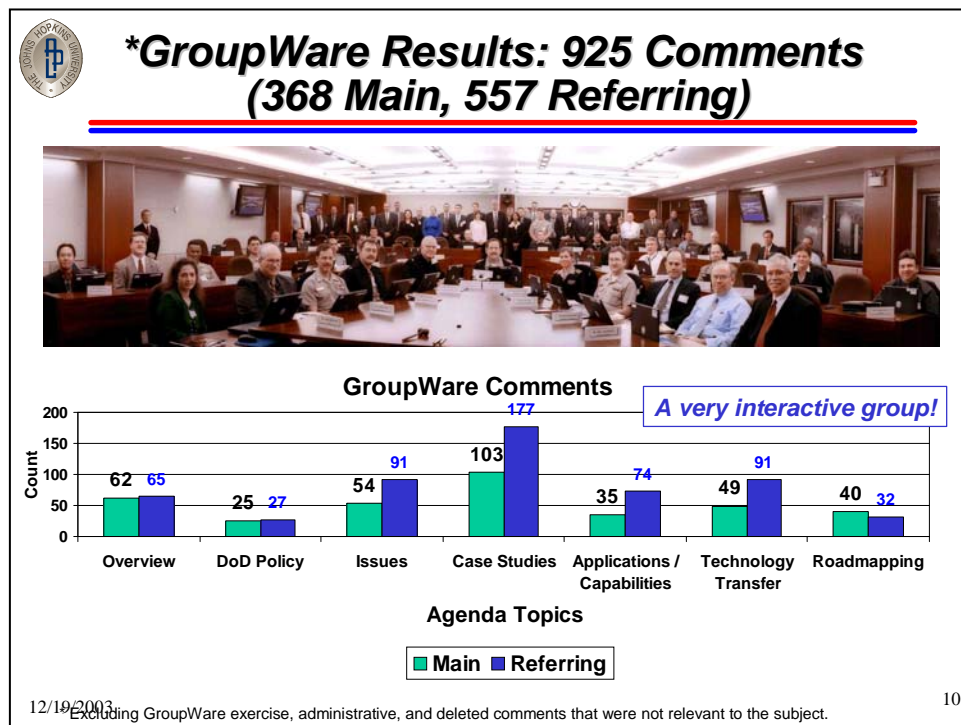


Figure 10: GroupWare Results: 925 Comments (368 Main, 557 Referring)

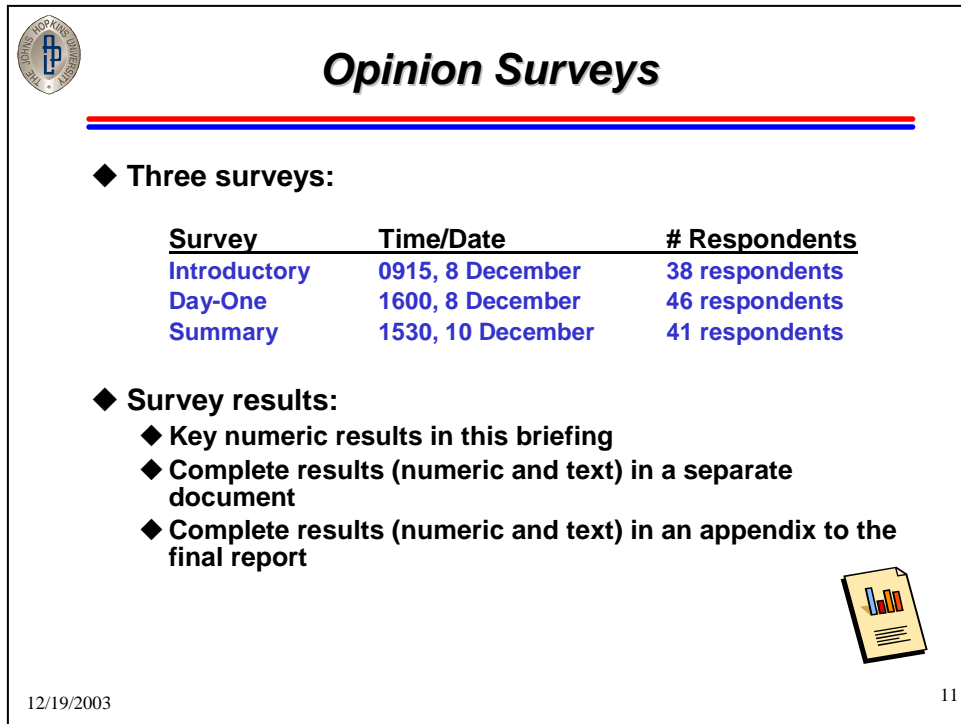


Figure 11: Opinion Surveys

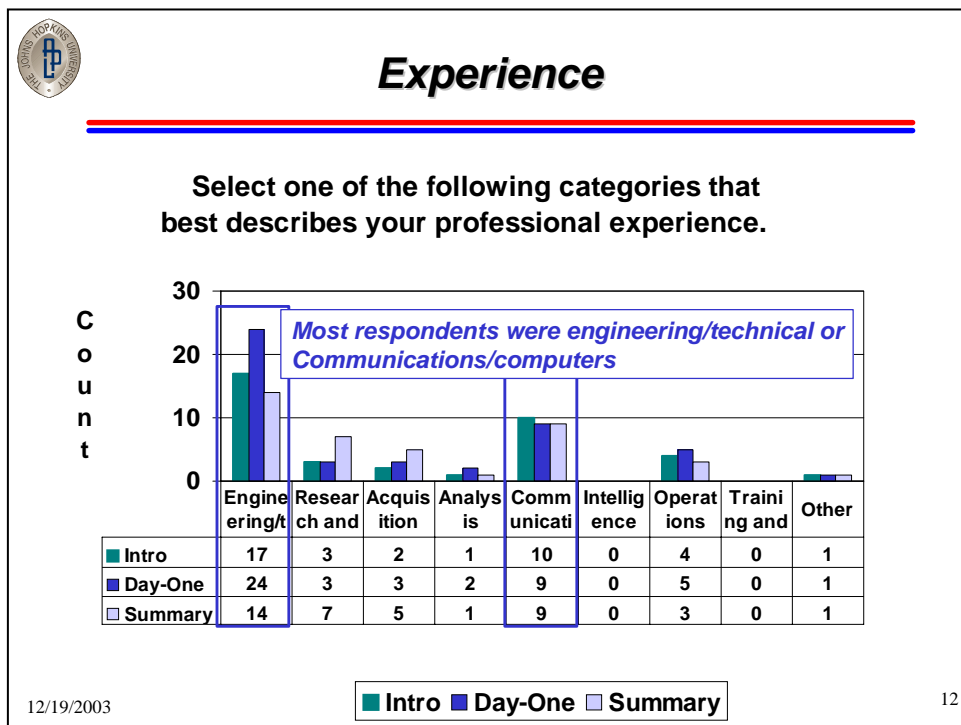


Figure 12: Experience



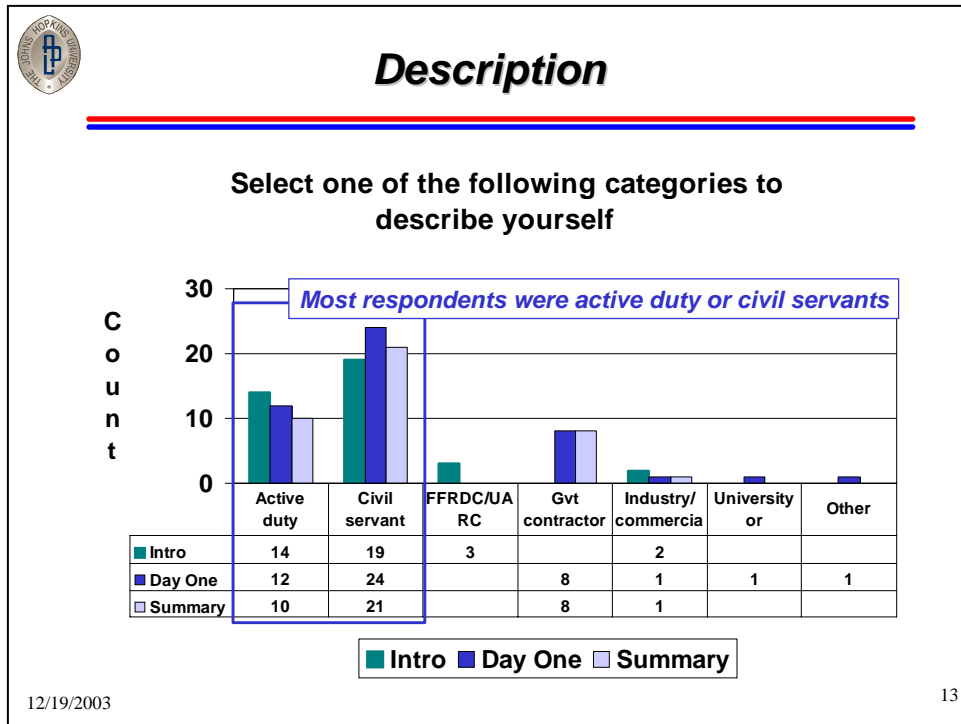


Figure 13: Description

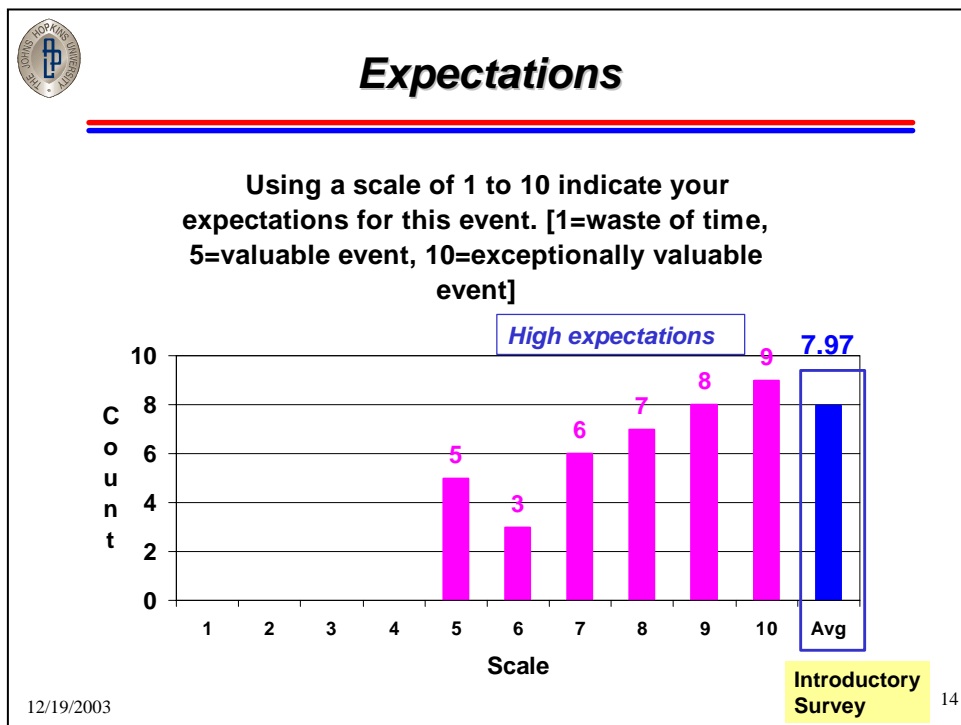


Figure 14: Expectations

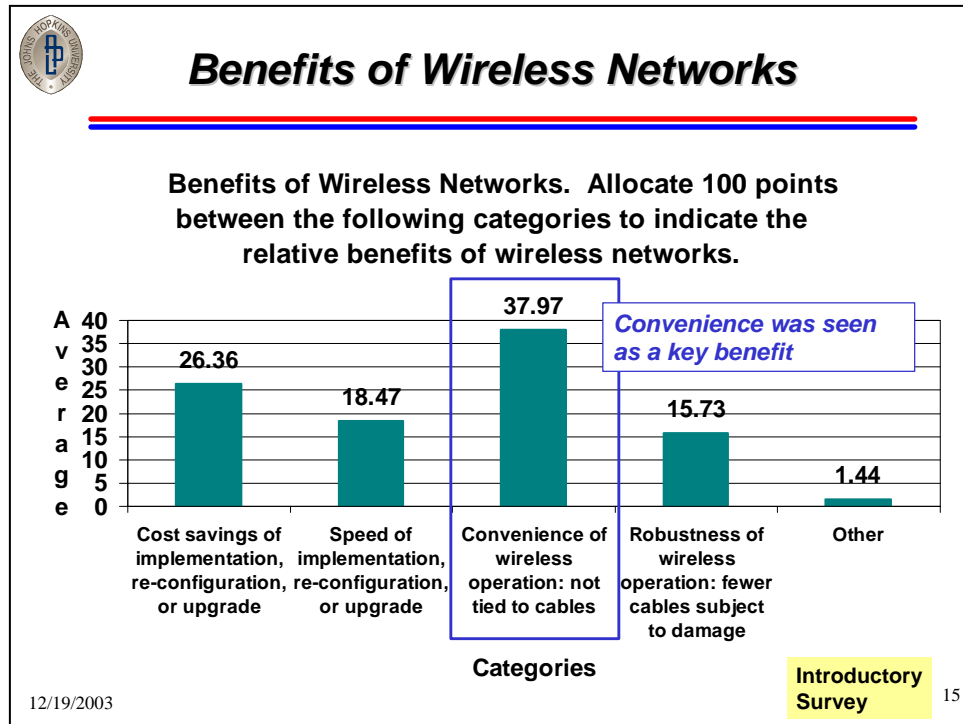


Figure 15: Benefits of Wireless Networks

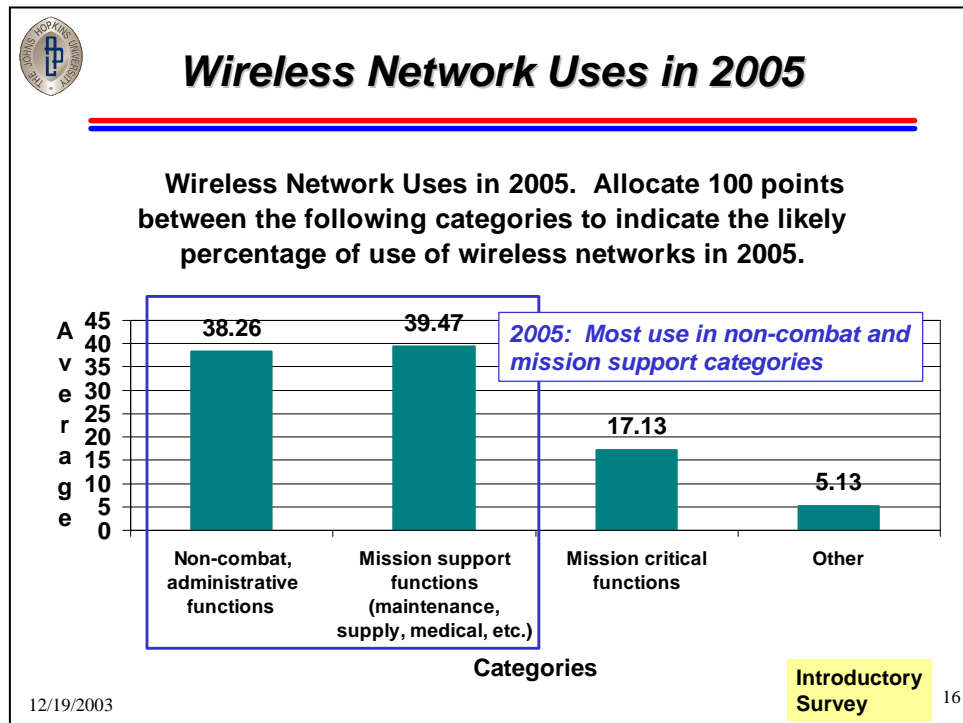


Figure 16: Wireless Network Uses in 2005

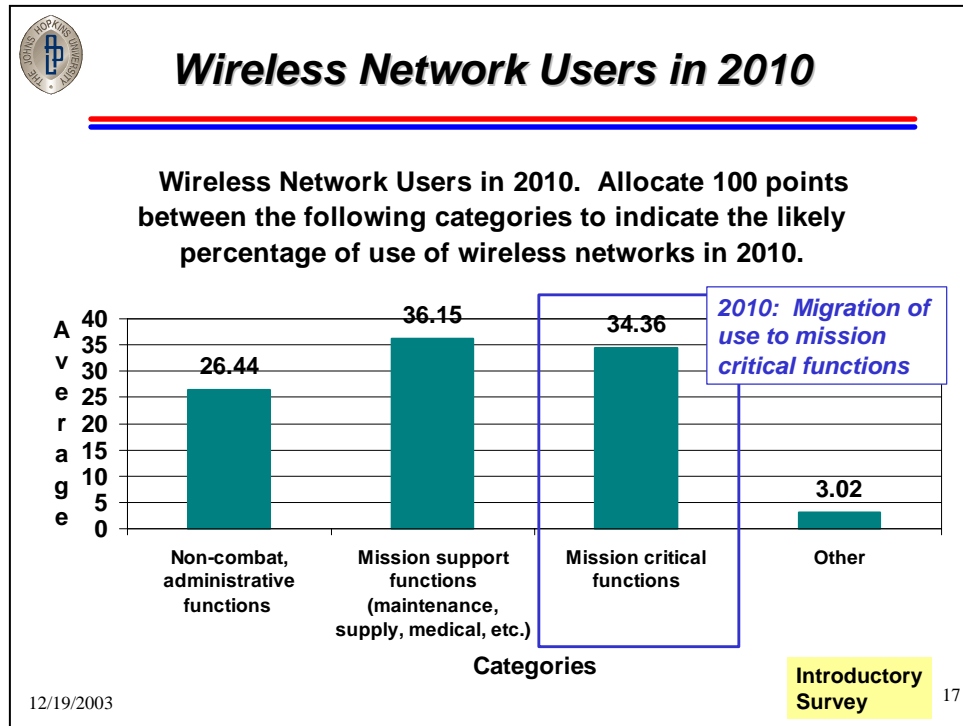


Figure 17: Wireless Network Users in 2010

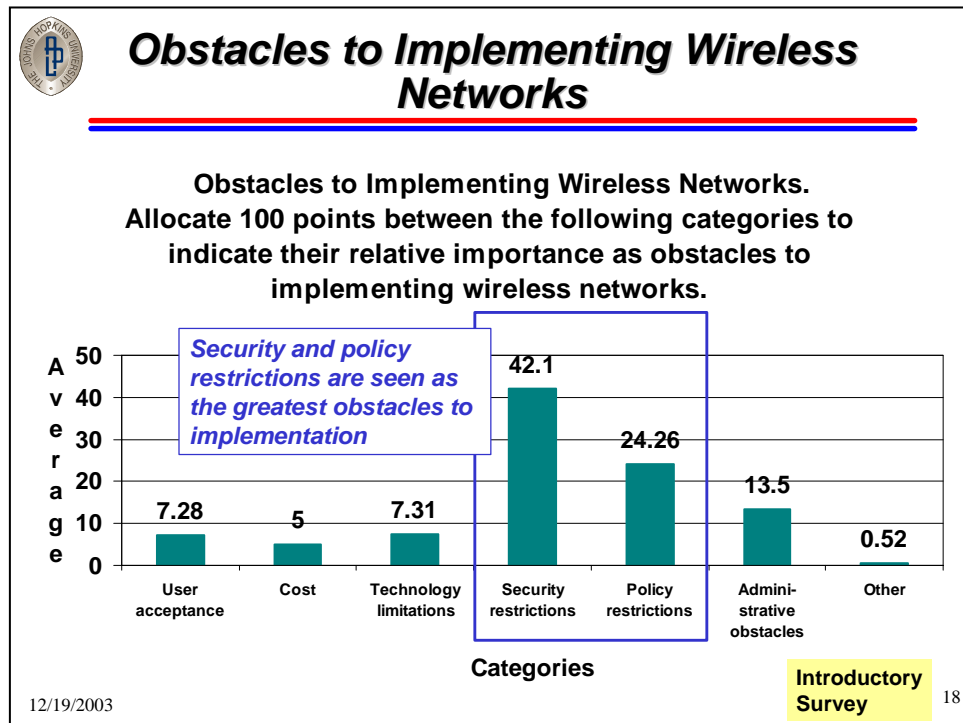


Figure 18: Obstacles to Implementing Wireless Networks

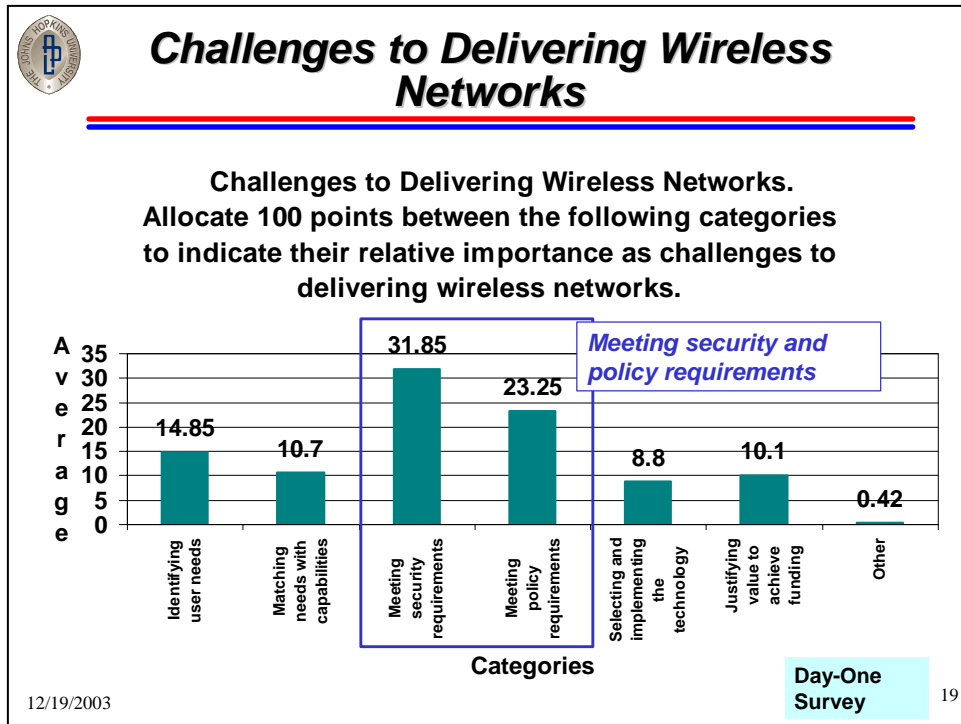


Figure 19: Challenges to Delivering Wireless Networks

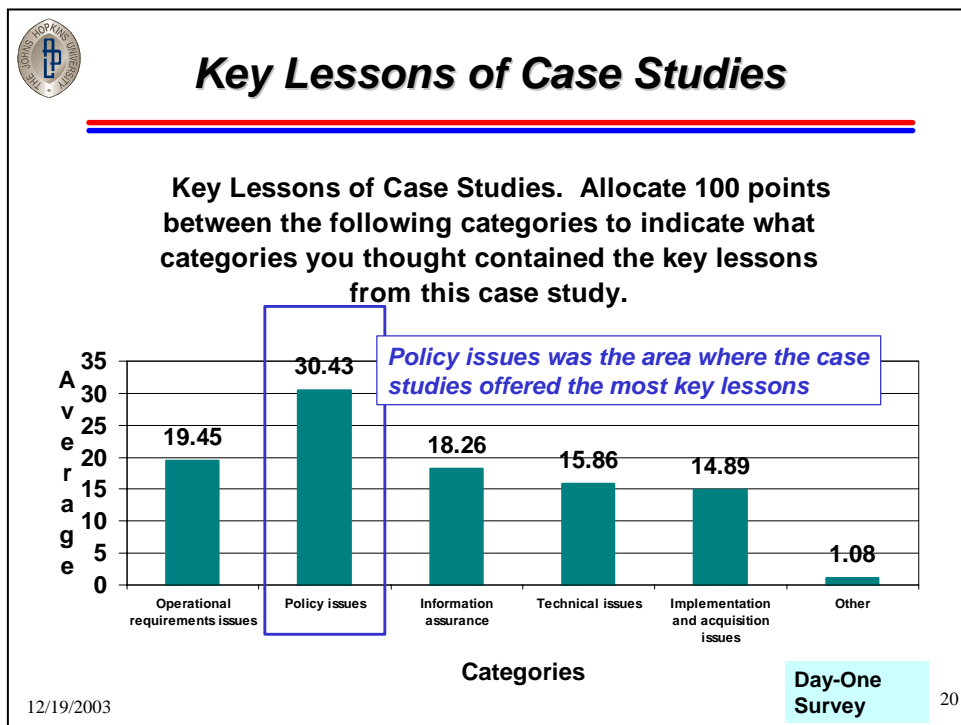


Figure 20: Key Lessons of Case Studies

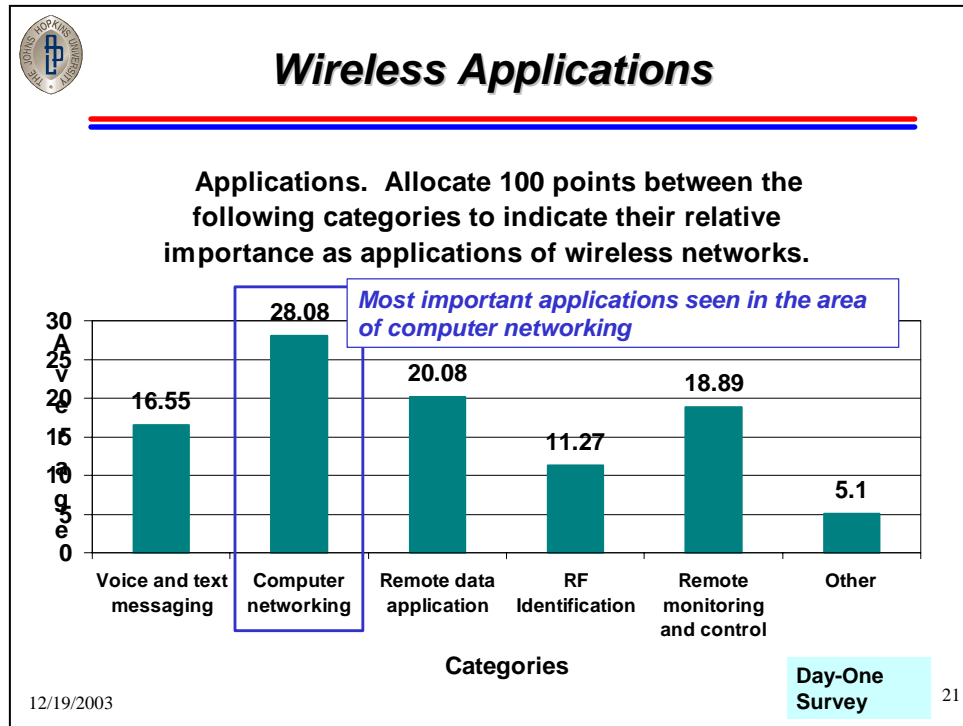


Figure 21: Wireless Applications

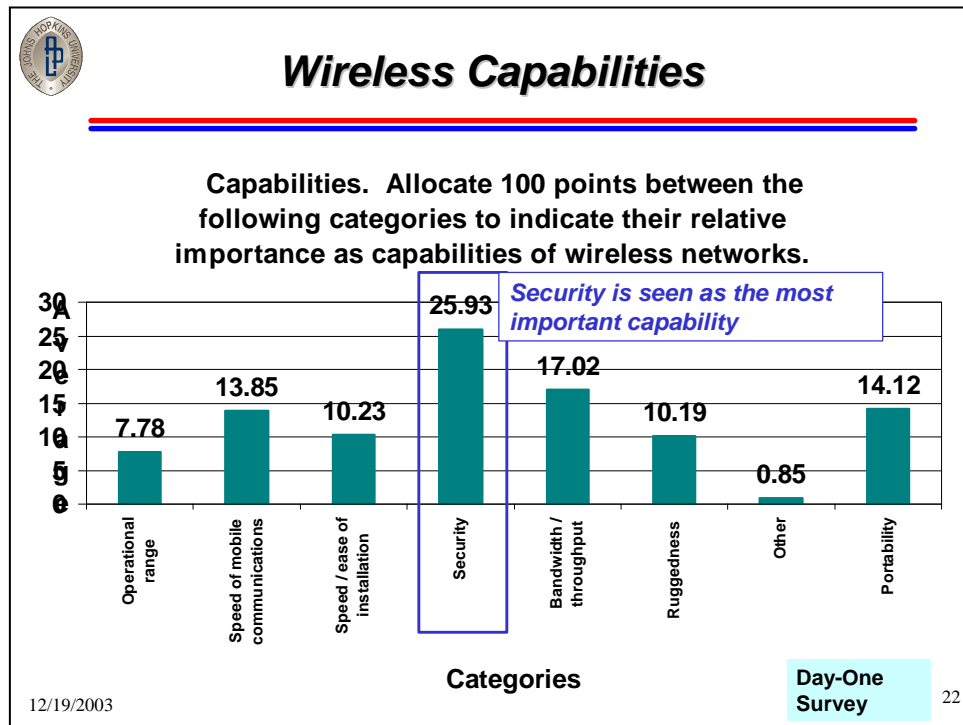


Figure 22: Wireless Capabilities

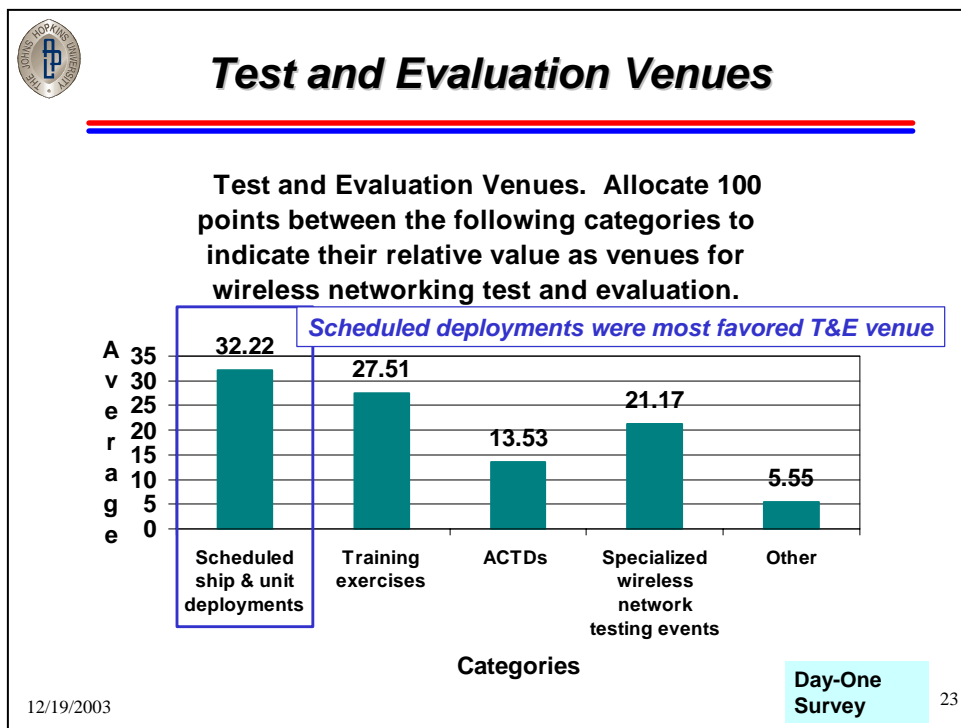


Figure 23: Test and Evaluation Venues

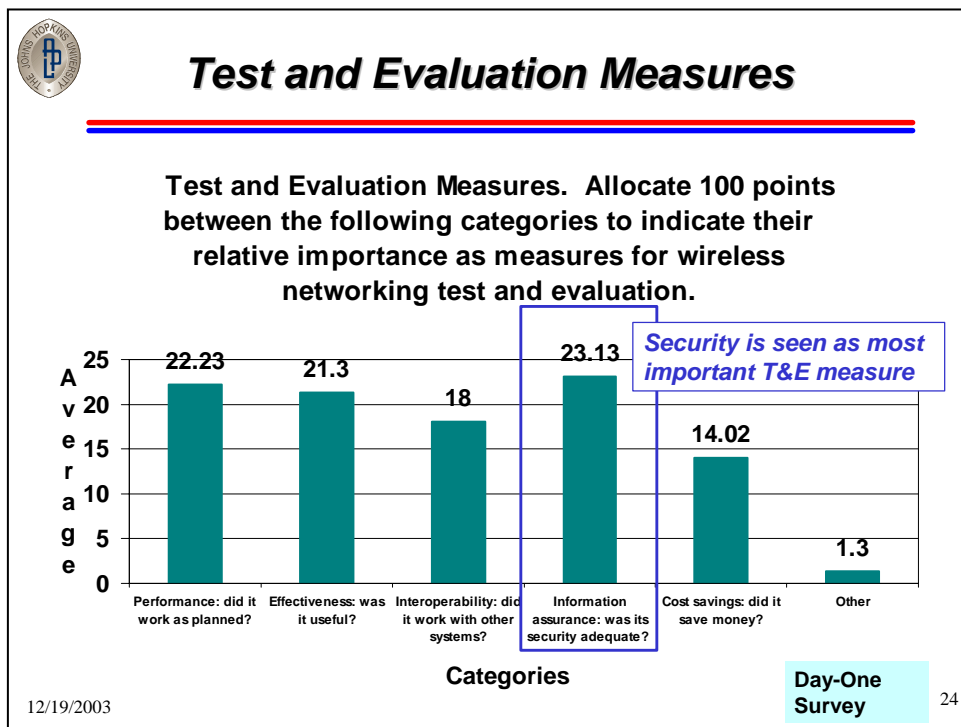


Figure 24: Test and Evaluation Measures

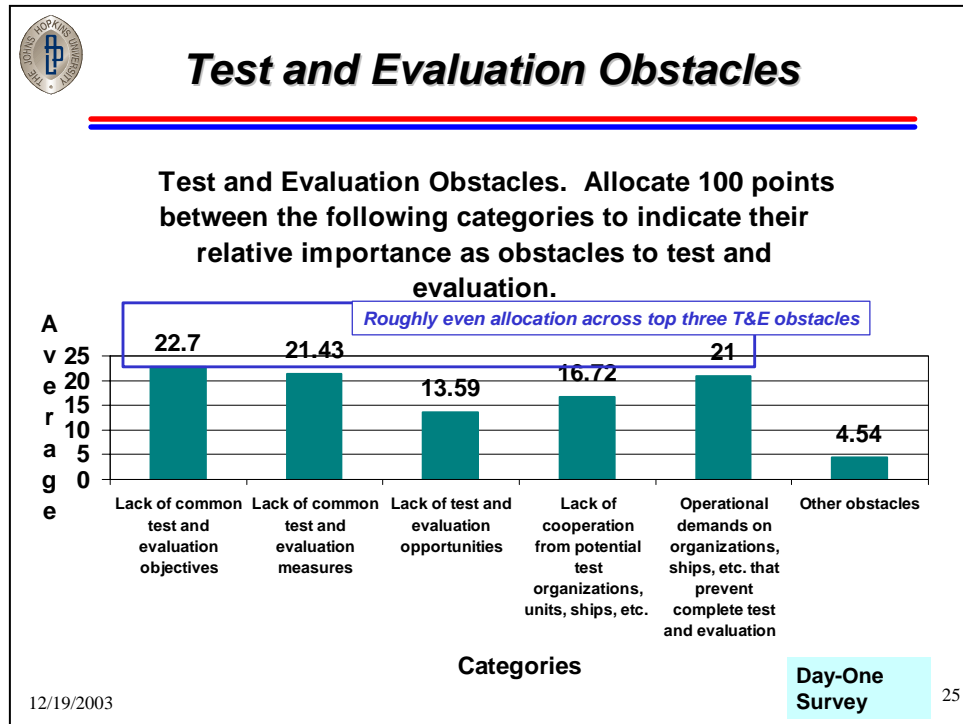


Figure 25: Test and Evaluation Obstacles

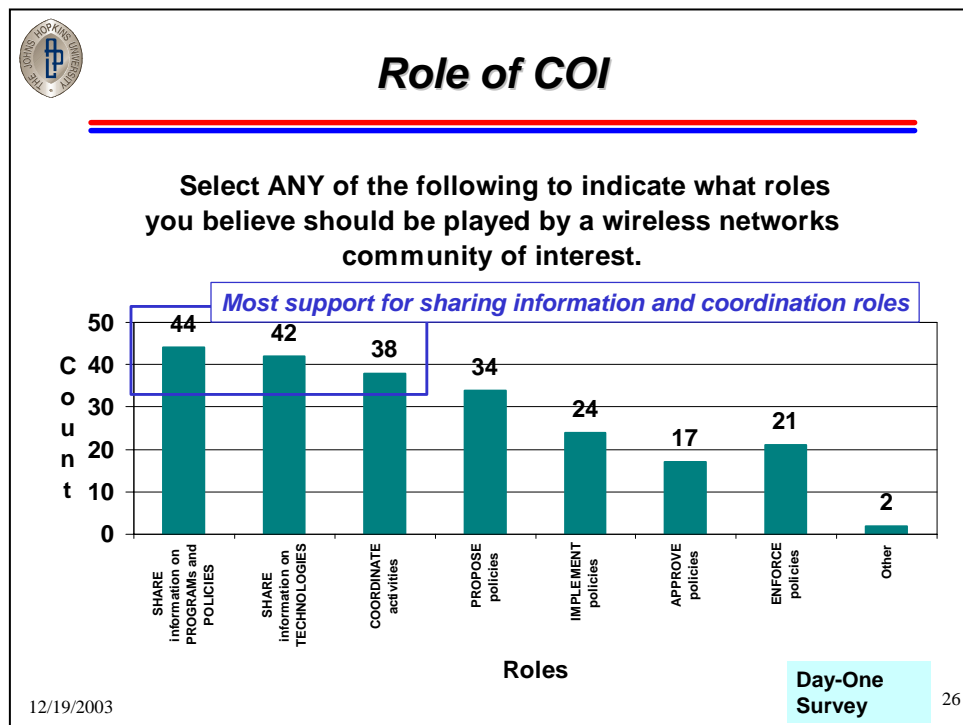


Figure 26: Role of COI

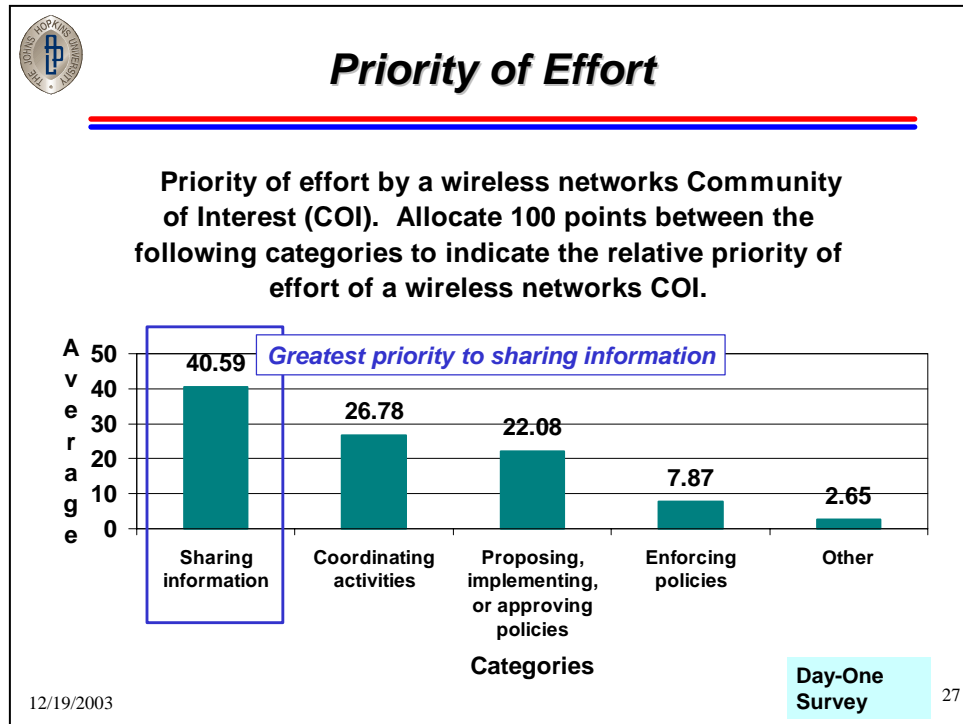


Figure 27: Priority of Effort

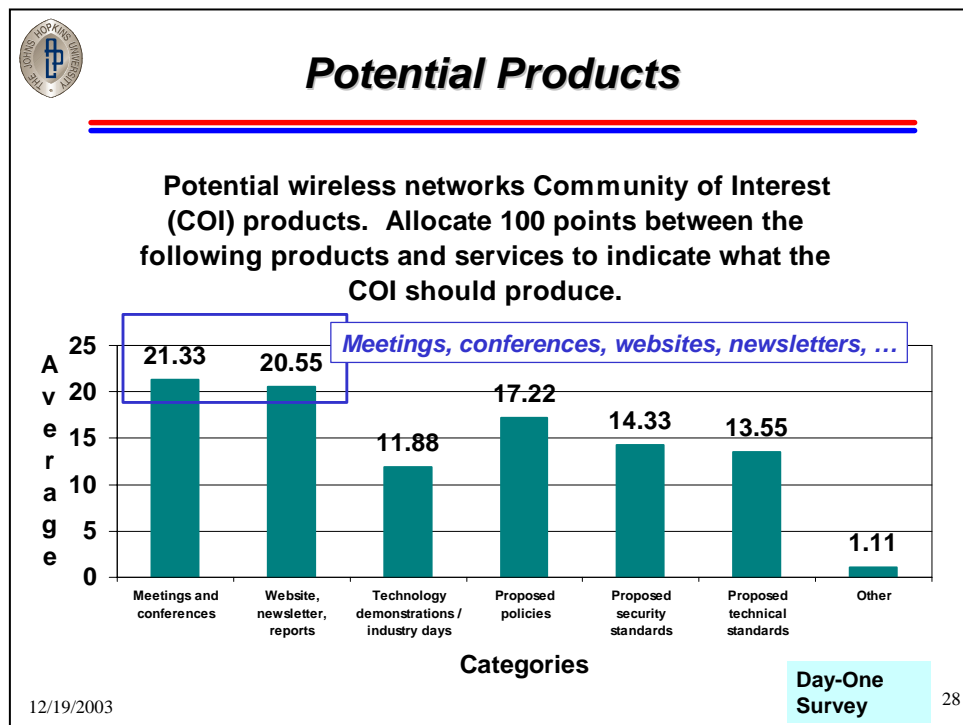


Figure 28: Potential Products



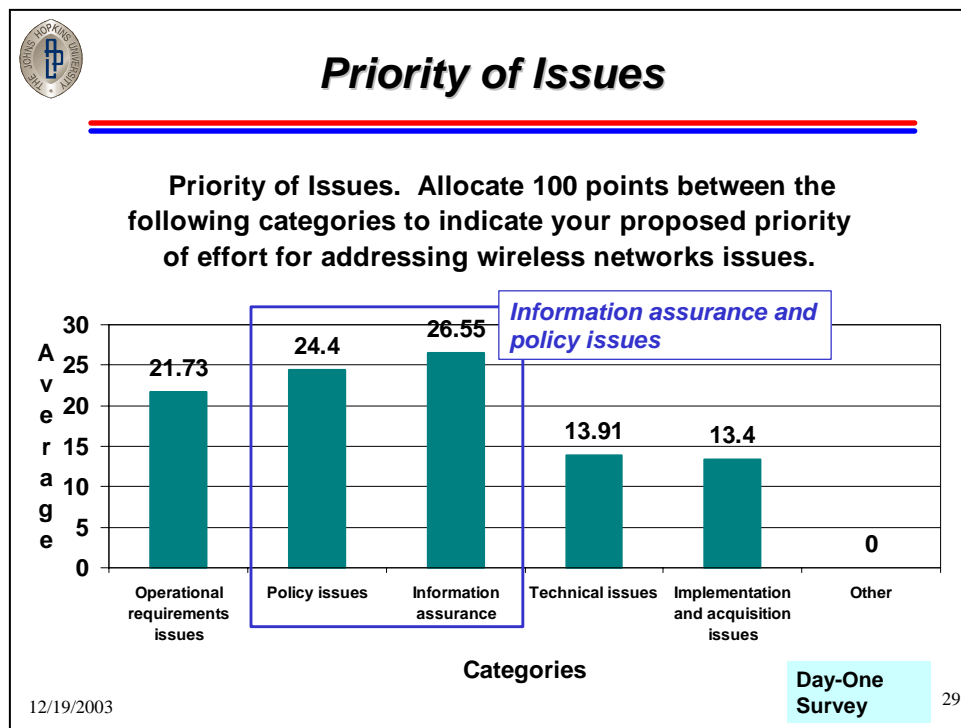


Figure 29: Priority of Issues

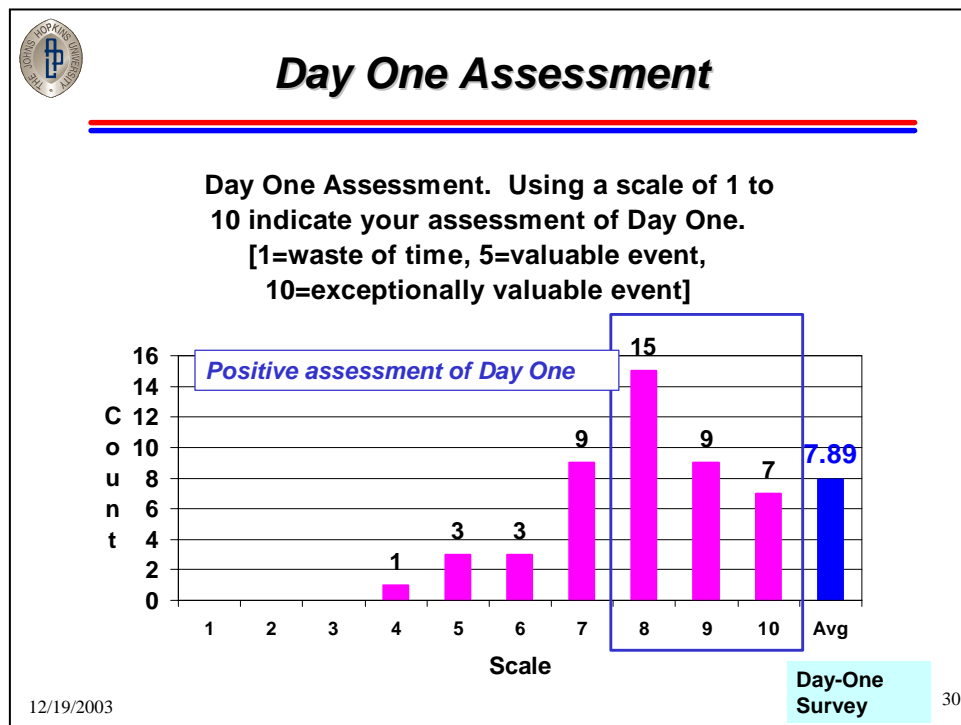


Figure 30: Day One Assessment

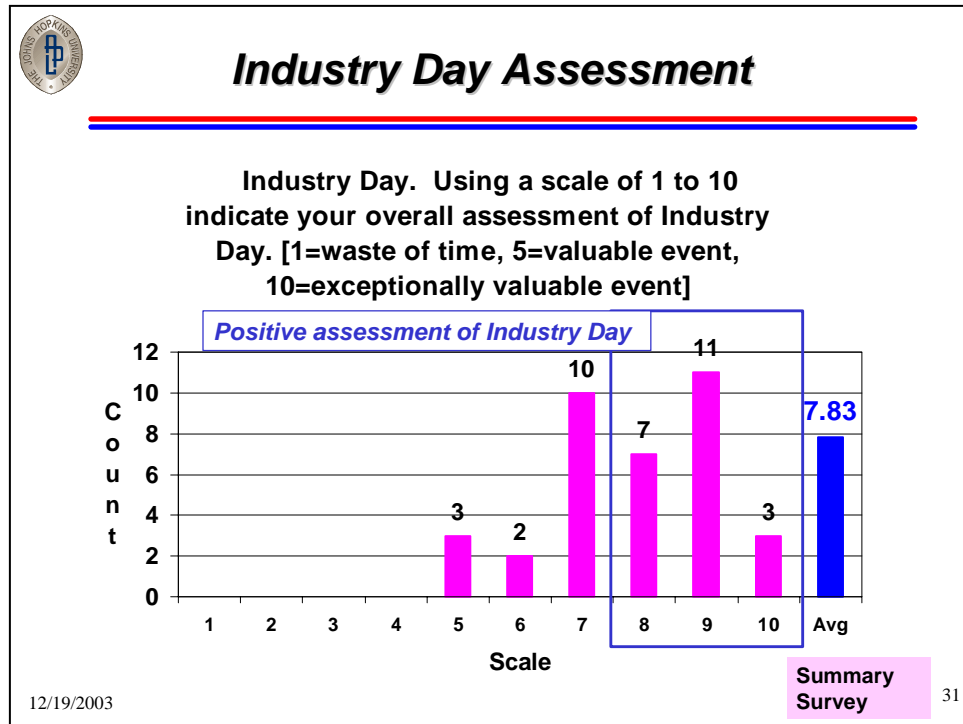


Figure 31: Industry Day Assessment

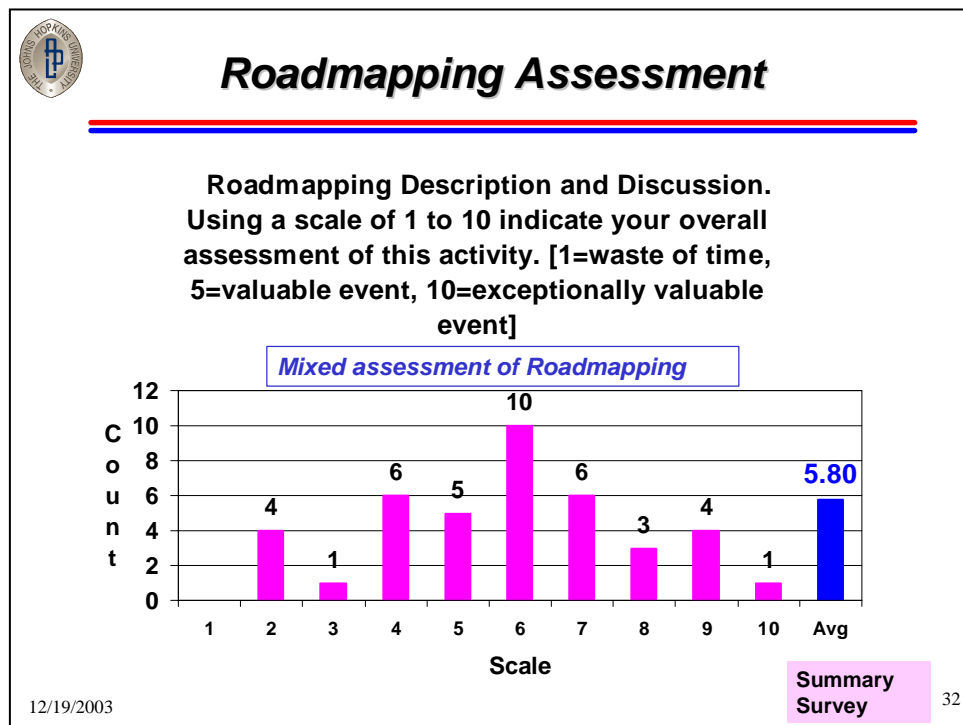


Figure 32: Roadmapping Assessment

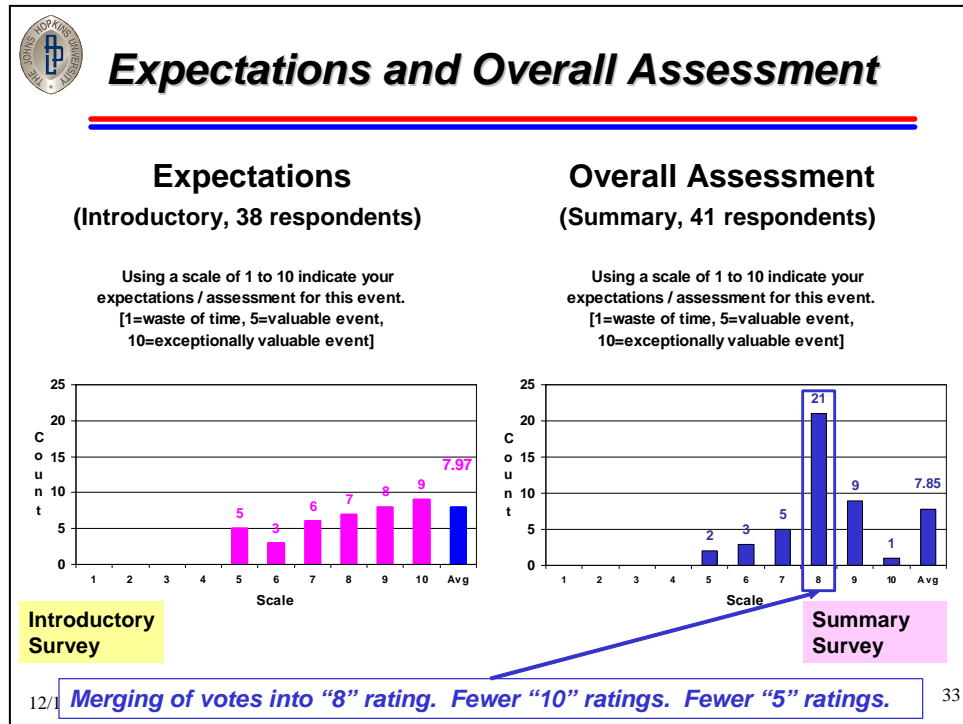


Figure 33: Expectations and Overall Assessment

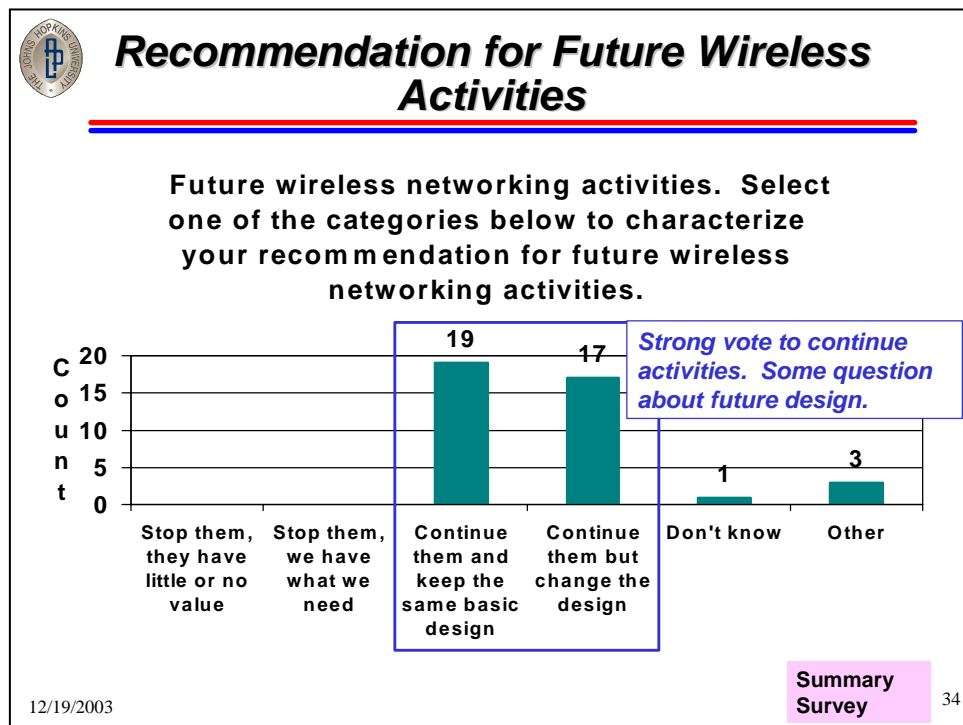


Figure 34: Recommendation for Future Wireless Activities

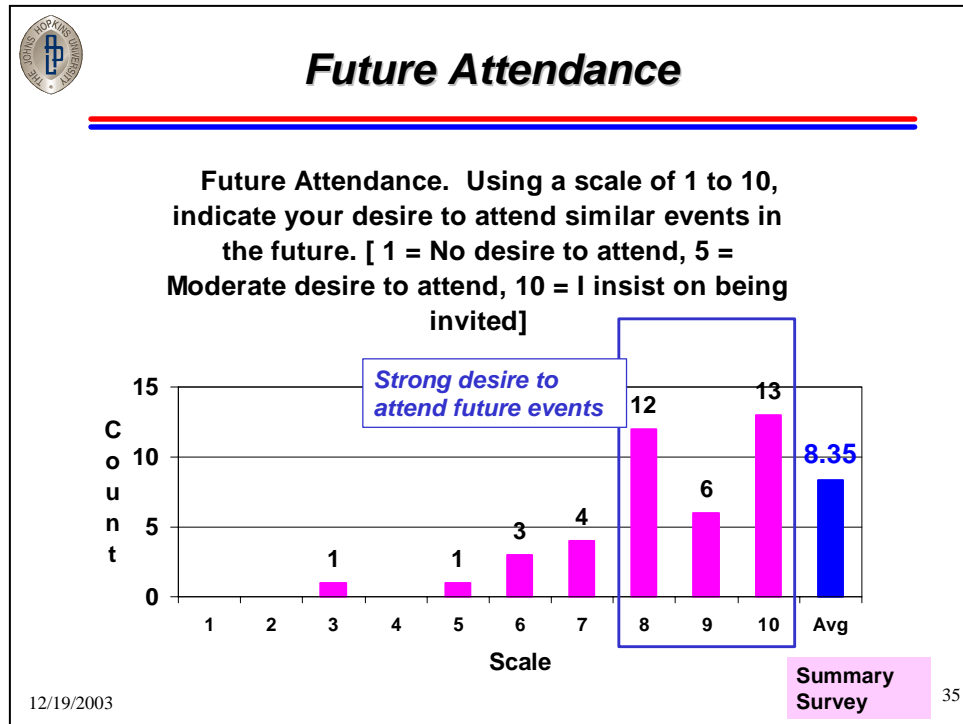


Figure 35: Future Attendance

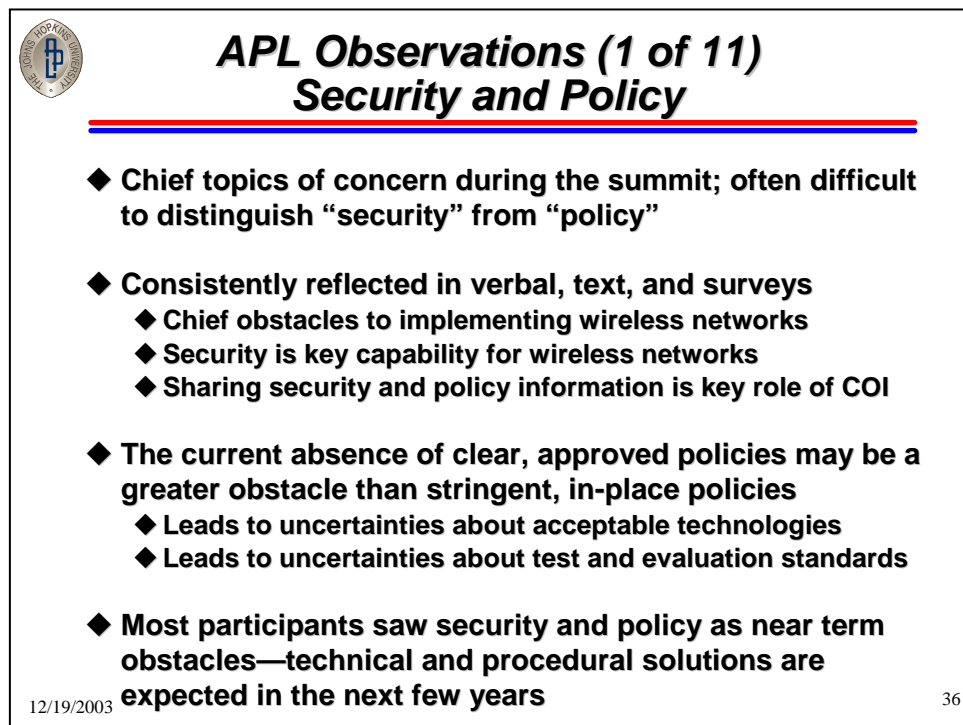



Figure 36: APL Observations (1 of 11)  
Security and Policy



### ***APL Observations (2 of 11)***


#### ***Need Documented Requirements***

---

- ◆ **To achieve funding, must have documented requirements**
- ◆ **WLAN implementation for submarine community appears much more mature than surface fleet. Lessons or insights?**
- ◆ **Several participants voiced the need for a “wireless champion” to push wireless technologies**
- ◆ **Discussions indicated that a clear business case has not been made for wireless**
  - ◆ **Benefits (cost savings, improved productivity, other mission enhancement or process improvement, ...)**
  - ◆ **Metrics**
  - ◆ **Justification of funding**

12/19/2003 37

Figure 37: APL Observations (2 of 11)  
Need Documented Requirements



### ***APL Observations (3 of 11)***


#### ***Wireless Networks Applications***

---

- ◆ **Some disagreement over the focus of applications and future development. Two basic approaches expressed:**
  - ◆ **A: Develop robust networks that can host to-be-developed applications**
    - Robust networks enable future, unknown applications
    - Users will identify applications they need
  - ◆ **B: Develop wireless “killer applications” that meet user needs and generate requirements**
    - Network capability is an enabler, not a clear requirement
    - Applications are basis of wireless business case
- ◆ **Most participants saw importance of both approaches**
  - ◆ **User demand & business case driven useful applications**
  - ◆ **Applications cannot deliver value without robust networks**
- ◆ **Few suggestions on specific new wireless applications**

12/19/2003 38

Figure 38: APL Observations (3 of 11)  
Wireless Networks Applications



### ***APL Observations (4 of 11)***


#### ***Wireless Networks Capabilities***

---

- ◆ **Most participants felt that capabilities highly dependent upon specific applications and user needs**
- ◆ **Discussion of capabilities addressed:**
  - ◆ **Six basic capabilities: 1-range, 2-speed of mobile communications, 3-speed and ease of installation, 4-security, 5-bandwidth/throughput, and 6-ruggedness**
  - ◆ **Participants suggested: interoperability, local CPU capacity, compatibility with other systems, supportability**
- ◆ **Security was rated the most important –reflected in most comments**
- ◆ **Adding requirements for ruggedness threatens the feasibility of using Commercial-off-the-shelf (COTS) products**

12/19/2003 39

Figure 39: APL Observations (4 of 11)  
Wireless Networks Capabilities



### ***APL Observations (5 of 11)***

#### ***Opportunities for Test and Evaluation***

---

- ◆ **Emphasis upon shipboard testing under actual conditions of use**
  - ◆ **Importance of identifying user needs and gaining user acceptance**
  - ◆ **Recognition of the scheduling and operational challenges involved in shipboard testing**
  - ◆ **Discussion of the use of USS Coronado as test site**
    - **Dedicated to meet such needs**
    - **Some concerns that other test environments needed**
- ◆ **Two principle obstacles to test and evaluation:**
  - ◆ **Absence of clear test and evaluation standards**
  - ◆ **Operational demands on ships, organizations, etc.**
- ◆ **Need to leverage test and evaluation results to reduce duplication of effort and cost**
- ◆ **Business case data should be collected during T&E**

12/19/2003 40

Figure 40: APL Observations (5 of 11)  
Opportunities for Test and Evaluation

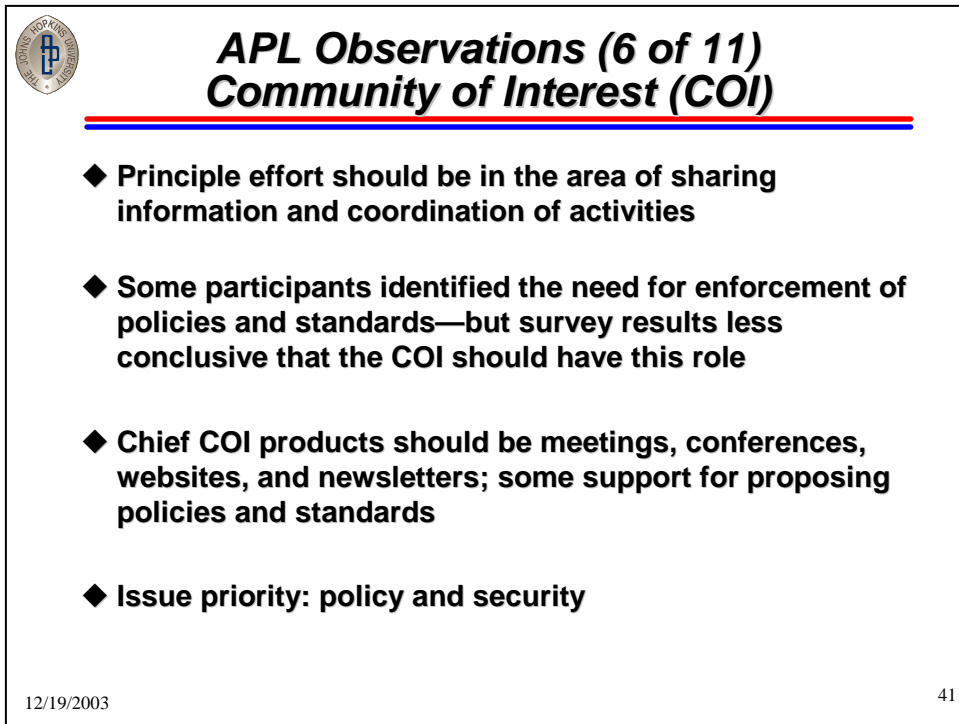


Figure 41: APL Observations (6 of 11)  
Community of Interest (COI)

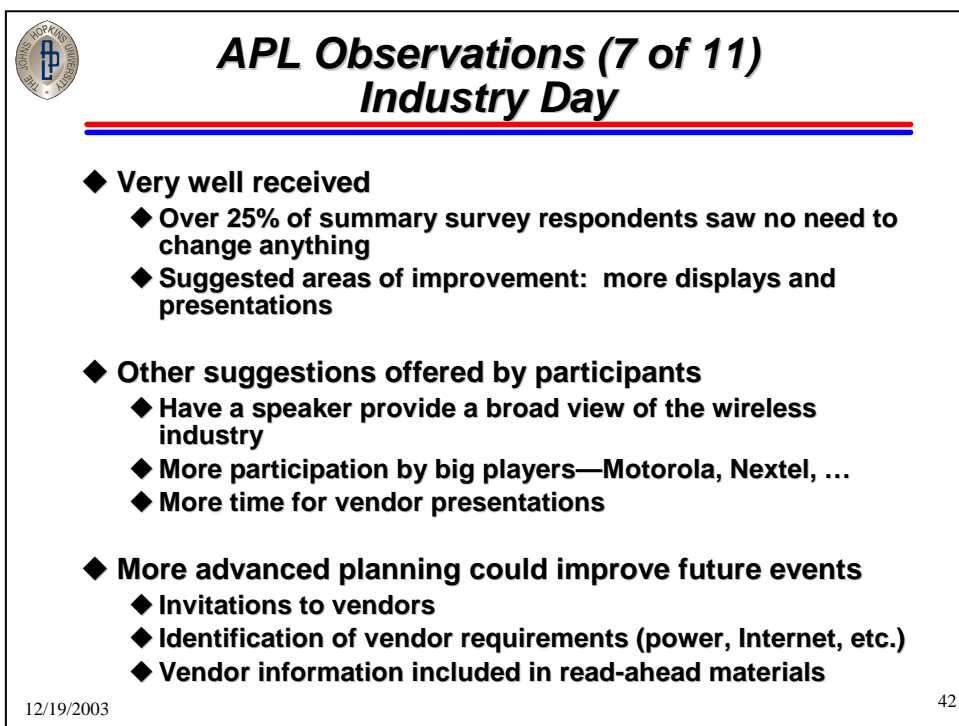



Figure 42: APL Observations (7 of 11)  
Industry Day



### ***APL Observations (8 of 11)***


#### ***Roadmapping***

---

- ◆ **Mixed assessment**
- ◆ **Seen as less valuable than other elements of the agenda**
- ◆ **Concerns stated by participants:**
  - ◆ **Good concept but insufficient data or analysis**
  - ◆ **Need for full participation to be effective**
  - ◆ **Problems with survey tool**
  - ◆ **Presentation focused on data collection, not roadmap development**
  - ◆ **Good process, but everyone needs access**
  - ◆ **Good tool, if every one contributes**
- ◆ **Product must show value to stakeholders**

12/19/2003 43

Figure 43: APL Observations (8 of 11)  
Roadmapping



### ***APL Observations (9 of 11)***

#### ***Additional Points***


---

- ◆ **Summit focused on 802.11 standards. Is this the full definition of “Wireless Networks”?**
- ◆ **Depending upon final security and policy solutions, user acceptance could become a more significant issue than indicated by this summit**
  - ◆ **Users may balk at perceived burdensome security steps**
  - ◆ **Wireless advantages could be lost in lengthy policy steps**
- ◆ **Need to understand threats to wireless networks. This summit was unclassified. Future events should address this issue.**

12/19/2003 44

Figure 44: APL Observations (9 of 11)  
Additional Points






### ***APL Observations (10 of 11) Additional Points (cont.)***

---

- ◆ Many saw wireless networks as just an extension of wired networks; others saw wireless networks as enabler of drastically lower costs and increased capabilities and productivity.
- ◆ Focus on near-term policies and security issues may have diverted attention from longer term issues
  - ◆ Exploration of high-value wireless applications
  - ◆ Requirements identification and documentation
  - ◆ Acquisition issues
- ◆ The cost savings of COTS products could be lost if security, policy, and added technical features push Navy needs beyond the envelope of COTS products
- ◆ Rapid turn-over in COTS may limit life-cycle savings

12/19/2003 45

Figure 45: APL Observations (10 of 11)  
Additional Points (cont.)




### ***APL Observations (11 of 11) Summit Design and Administration***

---

- ◆ Administrative procedures
  - ◆ Many participants did not register on the Web site
  - ◆ Some problems with sending/receiving clearance information
- ◆ Case studies were well received
  - ◆ Some benefit from more standardized format
  - ◆ Some basic information not always given (location, date, POC)
- ◆ Industry Day was well received
  - ◆ High approval for basic design
  - ◆ Some fine tuning could improve future efforts
- ◆ Topic discussions
  - ◆ Addressed specific event objectives
  - ◆ Not certain of value beyond a few general observations
- ◆ Roadmapping—conceptual v. practical

12/19/2003 46

Figure 46: APL Observations (11 of 11)  
Summit Design and Administration



## **Summary**

---

- ◆ **The Wireless Networks summit accomplished its objectives**
- ◆ **Need to put summit results in perspective: This was the first attempt to gather the Naval Wireless Networks Community of Interest**
- ◆ **Future events should address specific COI issues**
  - ◆ **Structure+**
  - ◆ **Role**
  - ◆ **Process**
  - ◆ **Products**
  - ◆ **Roadmap**
  - ◆ **...the way ahead**

12/19/2003 47

Figure 47: Summary

## APPENDIX E

### Introductory Survey Results Wireless Networks Summit, 8-10 December 2003

#### 1. Select one of the following categories that best describes your professional experience.

(Choose one.)

	Count
<b>Engineering/technical</b>	<b>19</b>
<b>Research and development</b>	<b>3</b>
<b>Acquisition</b>	<b>2</b>
<b>Analysis</b>	<b>1</b>
<b>Communications / computers</b>	<b>10</b>
<b>Intelligence</b>	<b>0</b>
<b>Operations</b>	<b>4</b>
<b>Training and doctrine</b>	<b>0</b>
<b>Other</b>	<b>1</b>

#### 2. Select ANY of the following categories to indicate your objectives for attending this event

(Choose up to 10.)

	Count
<b>Learn more about the Navy's approach to wireless networking</b>	<b>27</b>
<b>Learn more about wireless networking CAPABILITIES and APPLICATIONS</b>	<b>19</b>
<b>Learn more about wireless networking TECHNOLOGIES</b>	<b>21</b>
<b>Learn more about wireless networking POLICY and SECURITY ISSUES</b>	<b>27</b>
<b>Learn more about the wireless networking Community of Interest (COI)</b>	<b>17</b>
<b>Join the wireless networking COI</b>	<b>15</b>
<b>Influence the selection of wireless networking TECHNOLOGIES</b>	<b>11</b>
<b>Influence the resolution of wireless networking POLICY and SECURITY ISSUES</b>	<b>22</b>
<b>Influence the Navy's approach to wireless networking</b>	<b>23</b>
<b>Other</b>	<b>1</b>

**3. Select one of the following categories to describe yourself**

(Choose one.)

	Count
Active duty military	14
Civil servant	19
FFRDC/UARC employee	3
Government contractor employee	0
Industry/commercial employee	2
University or academic employee	0
Other	0

**4. Select one of the following categories to describe your relationship to wireless networking**

(Choose one.)

	Count
Current program manager (manage/support manager of a current wireless program)	14
Current user (use of a wireless network)	1
Current stakeholder (have a vested interest in a current wireless network)	4
Current implementer or acquirer	6
Potential program manager	0
Potential user	1
Potential stakeholder	3
Potential implementer or acquirer	2
Policy maker	6
Other	1

**5. Benefits of Wireless Networks. Allocate 100 points between the following categories to indicate the relative benefits of wireless networks.**

(Allocate all resources.)

**2.1. Cost savings of implementation, re-configuration, or upgrade**

Low	High	Avg	Med.		#
5	75	26.36	25		38

**2.2. Speed of implementation, re-configuration, or upgrade**

Low	High	Avg	Med.		#
5	50	18.47	20		38

**2.3. Convenience of wireless operation--not tied to cables**

Low	High	Avg	Med.		#
10	95	37.97	35		38

**2.4. Robustness of wireless operation--fewer cables subject to damage**

Low	High	Avg	Med.		#
5	60	15.73	15		38

**2.5. Other**

Low	High	Avg	Med.		#
5	20	1.44	0		38

**6. Wireless Network Uses in 2005. Allocate 100 points between the following categories to indicate the likely percentage of use of wireless networks in 2005.**

(Allocate all resources.)

**2.6. Non-combat, administrative functions**

Low	High	Avg	Med.		#
10	89	38.26	45		38

**2.7. Mission support functions (maintenance, supply, medical, etc.)**

Low	High	Avg	Med.		#
10	100	39.47	40		38

**2.8. Mission critical functions**

Low	High	Avg	Med.		#
1	60	17.13	20		38

**2.9. Other**

Low	High	Avg	Med.		#
10	80	5.13	0		38

**7. Wireless Network Users in 2010. Allocate 100 points between the following categories to indicate the likely percentage of use of wireless networks in 2010.**

(Allocate all resources.)

**2.10. Non-combat, administrative functions**

Low	High	Avg	Med.		#
10	75	26.44	30		38

**2.11. Mission support functions (maintenance, supply, medical, etc.)**

Low	High	Avg	Med.		#
15	100	36.15	33		38

**2.12. Mission critical functions**

Low	High	Avg	Med.		#
10	100	34.36	30		38

**2.13. Other**

Low	High	Avg	Med.		#
10	30	3.02	0		38

**8. Obstacles to Implementing Wireless Networks. Allocate 100 points between the following categories to indicate their relative importance as obstacles to implementing wireless networks.**

(Allocate all resources.)

**2.14. User acceptance**

Low	High	Avg	Med.		#
2	25	7.28	5		38

**2.15. Cost**

Low	High	Avg	Med.		#
5	20	5	0		38

**2.16. Technology limitations**

Low	High	Avg	Med.		#
3	30	7.31	0		38

**2.17. Security restrictions**

Low	High	Avg	Med.		#
20	85	42.1	40		38

## Appendix E, Introductory Survey Results

### 2.18. Policy restrictions

Low	High	Avg	Med.		#
10	50	24.26	25		38

### 2.19. Administrative obstacles (complexity/length of approval process)

Low	High	Avg	Med.		#
5	33	13.5	15		38

### 2.20. Other

Low	High	Avg	Med.		#
5	15	0.52	0		38

### 9. Using a scale of 1 to 10 indicate your expectations for this event. [1=waste of time, 5=valuable event, 10=exceptionally valuable event]

(Rate from 1 to 10, with 10 the highest value.)

1	2	3	4	5	6	7	8	9	10	Total
0	0	0	0	5	3	6	7	8	9	38

### 10. Using a scale of 1 to 10, indicate your expected influence on this event. [1 = no influence, 5 = moderate influence, 10 = significant influence]

(Rate from 1 to 10, with 10 the highest value.)

1	2	3	4	5	6	7	8	9	10	Total
0	1	1	5	14	3	6	3	4	1	38

Intentionally Left Blank



## APPENDIX F

### Day One Survey Results Wireless Networks Summit, 8-10 December 2003

#### 1. Select one of the following categories that best describes your professional experience.

(Choose one.)

	Count
<b>Engineering/technical</b>	<b>24</b>
<b>Research and development</b>	<b>3</b>
<b>Acquisition</b>	<b>3</b>
<b>Analysis</b>	<b>2</b>
<b>Communications / computers</b>	<b>9</b>
<b>Intelligence</b>	<b>0</b>
<b>Operations</b>	<b>5</b>
<b>Training and doctrine</b>	<b>0</b>
<b>Other</b>	<b>1</b>

#### 2. Select ANY of the following categories to indicate your objectives for attending this event

(Choose up to 10)

	Count
<b>Learn more about the Navy's approach to wireless networking</b>	<b>29</b>
<b>Learn more about wireless networking CAPABILITIES and APPLICATIONS</b>	<b>24</b>
<b>Learn more about wireless networking TECHNOLOGIES</b>	<b>23</b>
<b>Learn more about wireless networking POLICY and SECURITY ISSUES</b>	<b>30</b>
<b>Learn more about the wireless networking Community of Interest (COI)</b>	<b>19</b>
<b>Join the wireless networking COI</b>	<b>10</b>
<b>Influence the selection of wireless networking TECHNOLOGIES</b>	<b>23</b>
<b>Influence the resolution of wireless networking POLICY and SECURITY ISSUES</b>	<b>27</b>
<b>Influence the Navy's approach to wireless networking</b>	<b>24</b>
<b>Other</b>	<b>3</b>

## Appendix F, Day One Survey Results

### 3. Select one of the following categories to describe yourself

(Choose one.)

	Count
Active duty military	12
Civil servant	24
FFRDC/UARC employee	0
Government contractor employee	8
Industry/commercial employee	1
University or academic employee	1
Other	1

### 4. Select one of the following categories to describe your relationship to wireless networking

(Choose one.)

	Count
Current program manager (manage/support manager of a current wireless program)	14
Current user (use of a wireless network)	1
Current stakeholder (have a vested interest in a current wireless network)	6
Current implementer or acquirer	9
Potential program manager	2
Potential user	0
Potential stakeholder	2
Potential implementer or acquirer	3
Policy maker	6
Other	3

### 5. Key Lessons of Case Studies. Allocate 100 points between the following categories to indicate what categories you thought contained the key lessons from this case study.

(Allocate all resources.)

#### 2.1. Operational requirements issues

Low	High	Avg	Med.		#
5	80	19.45	15		46

#### 2.2. Policy issues

Low	High	Avg	Med.		#
10	80	30.43	30		46

## Appendix F, Day One Survey Results

### 2.3. Information assurance

Low	High	Avg	Med.		#
5	75	18.26	15		46

### 2.4. Technical issues

Low	High	Avg	Med.		#
5	90	15.86	10		46

### 2.5. Implementation and acquisition issues

Low	High	Avg	Med.		#
5	75	14.89	10		46

### 2.6. Other

Low	High	Avg	Med.		#
10	40	1.08	0		46

6. Please describe what you thought were the key lessons from the case studies. If you allocated points to "Other," please describe what category you had in mind.

(Click in the box to enter text.)

#	Comment
1	The challenge associated with accrediting the networks.
2	We need a WIRELESS Champion for the Navy and DoD. Cannot continue to suffer all this pain and expense each time we review new wireless technologies, applications or specific architectures.
3	The process of obtaining required certifications is time consuming and much more involved than for a wired network.
4	The key point in my mind was the difficulty in implementing WLAN with the current lack of substantive guidance from any authoritative source.
5	Testing issues - difficulties in characterizing tests Schedule slippages in getting certifications Determining numbers of access points for a ship Bandwidth management Crypto key updating issues - for classified WLAN TEMPEST/HERO/HERF/HERP/EMI/EMC
6	Realization that everyone has the same issues regarding policy, security, and acquisition.  Realization not everyone understands 8500 and Common criteria

## Appendix F, Day One Survey Results

7	Policy issues and new requirements. TTP and CONOPS are still probably the most important issues along with policy and security now that I know more about the state of emerging technology.
8	They provided a good background on what was needed from a certification process on implementing a WLAN. They also provided good lessons learned to some of the obstacles that could be encountered in implementing a WLAN.
9	Policy to minimize duplication of accreditation lacking
10	Too much effort is being spent on redundant efforts, the wireless effort needs focus!
11	Technology is in place. The Navy is applying requirement over and beyond industry. This is a need addition. However, we are not going about the process smartly
12	Policy issues and decisions drive the actual technical solutions that are approved and fielded. Information Assurance provide the framework for providing a robust, secure and comprehensive wireless network solution.
13	Cost of implementing wireless will be higher than anticipated and may obviate return on investment advantages.
14	security issues facing all projects, and approval and accreditation process
15	No one has managed to field a system that is completely approved for unclass and class use.
16	Time to certification
17	1. IA was planned into the implementation of the case studies 2. User requirements were evaluated 3. Many lessons learned were derived and need to be shared amongst the COI
18	Insertion of WLAN technology on ship. Learning the IA issues that need to be addressed in order for the technology to move from an experiment to full deployment.
19	I felt it was evident from the case studies that technology is there today to do wireless LANS aboard ships, but just because technology is ready does not mean it is a smart thing to do in all cases. Critical issues like compatibility and clearly defined requirements MUST be taken into account.
20	Learning about the various approvals required, that it's more than FIPS 140.
21	Case studies highlighted what the integration issues are for these devices and the current limits of the policy. The IA concerns are known and the technology is maturing, so the issues are how we implement this technology.
22	IA was a major concern in the chat during the case study presentations.
23	Since I was mostly unaware of these issues just the background was new to me. I learned quite a bit from each case study.

## Appendix F, Day One Survey Results

24	Information on ICAS
25	The requirements seemed to be the main issue the Navy is researching. The proper entities, policies and regulations provided by the case studies, lack much Joint 'Flavor', however GIG was mentioned, demonstrating outer interoperability and compliance concerns.  IA is also a great concern followed by bandwidth, this is an across issue with all services. Other services architecture was not included in a accent mode, such as JTRS and WIN-T.
26	It's very difficult to get one of these projects "online".
27	Case studies showed the difficulties in implementing new programs. They also showed how bureaucracy can slow down deployment of new technology.
28	process for installations however, there is still no documented process for how to move forward, only these examples.
29	sec 11 findings..... along security/of hardware and key management issues it brings to wireless network.

### 7. Case Study Improvement. Select any of the following categories to indicate ways in which to improve the case studies.

(Choose up to the maximum number of selections.)

	Count
No improvements needed (NOTE: please select no other choices)	15
Provide MORE information on POLICY issues	14
Provide LESS information on policy issues	0
Provide MORE information on TECHNICAL issues	18
Provide LESS information on TECHNICAL Issues	1
Other	4
Provide MORE information on ACQUISITION / IMPLEMENTATION issues	16
Provide LESS information on ACQUISITION / IMPLEMENTATION issues	0

### 8. Please explain your answer on how to improve the case studies. If you selected the "Other" category, please describe what category you had in mind.

(Click in the box to enter text.)

#	Comment
1	I would have liked to see more details on the challenges of accreditation.
2	make sure briefer has the presentation that he sent.

## Appendix F, Day One Survey Results

3	At this point in time - the case studies were appropriate- they outlined all the reasons why we need 1 navy policy. In the future there may be a need for more technical or application/implementation issues... but there are currently no POR programs to baseline from.
4	I am personally interested in the technical details and results of testing.
5	It would be great to have a Knowledge Portal for all of these issues where a user could get any pertinent information, organizations, POC's etc. in a single stop.
6	More details on what was implemented in the architecture - IDS, VPN, etc
7	Provide a separate brief for technical only audience. Also, include process on how to go about executing program. Case studies were just fine but a little more technical and architectural background might have been helpful. I am more of a fleet operator.
8	Would like to know the specific organizations the cases were dealing with to acquire accreditation
9	I think the case studies we good to a point, they needed to provide more how and why they did what they did. If it was available they should refer us to a web site to disclose this type of information.
10	More coordination is needed across the cases to increase the knowledge on certain variables, security solutions, etc.
11	More focus on lessons learned from policy issues and technical issues. So that individuals will not repeat the same mistakes.
12	hold all case studies to same format
13	Need more information on what kinds of design and implementation issues arose, what advantages were observed, what the objective of the installation was and whether objectives were met.
14	More specifics on why a particular policy slowed down the deployment process or added costs to a project.
15	How did the current state of the DoD policy impact implementation decisions?
16	Need further validated information on IA issues which bridges the technical issues with policy
17	Provide Points of Contact or Web sites for further information.
18	n/a
19	The case studies were fine, they highlighted what the issues are.
20	We need to look more at usage policy and getting the systems into the acquisition pipeline.
21	No entry
22	I would like more information on technical limitations
23	More Jointness and GIG assessment, testing and research should be used.
24	Some people were confused as to which technologies are employed in 802.11x and the security issues affecting them.
25	Security issues also important

**9. Applications. Allocate 100 points between the following categories to indicate their relative importance as applications of wireless networks.**

(Allocate all resources.)

**2.7. Voice and text messaging**

Low	High	Avg	Med.		#
5	75	16.55	20		47

**2.8. Computer networking**

Low	High	Avg	Med.		#
10	75	28.08	25		47

**2.9. Remote data application**

Low	High	Avg	Med.		#
5	70	20.08	20		47

**2.10. RF Identification**

Low	High	Avg	Med.		#
5	50	11.27	10		47

**2.11. Remote monitory and control**

Low	High	Avg	Med.		#
5	75	18.89	20		47

**2.12. Other**

Low	High	Avg	Med.		#
10	100	5.1	0		47

**10. Please explain your answer on applications. If you selected the "Other" category, please describe what category you had in mind.**

(Click in the box to enter text.)

#	Comment
1	Every single one of these choices can benefit from wireless implementation.
2	Shipboard environments mean MOBILITY requirements. As manning decreases - communications between individual and the available data become critical. Cannot afford to be static and cannot rely on single point of entry for the information exchange or collaboration. Need the mobile networks for voice and data.

## Appendix F, Day One Survey Results

3	WLAN need to fill the gap in areas of the ship and remote sites that currently do not enjoy access to network resources.
4	RFID is needed to track movement of material and weapons throughout the ship for strike up/down, remote monitoring/control will be necessary enabler for wide spread utilization of conditioned based maintenance in shipboard equipment, voice/text add to quality of service, computer networking may only be really needed for accommodating users who are continually on the move. Most users would likely be at a fixed workstation.
5	With limitation on bandwidth this drives the need to capture and document what is required for today's operation in terms of voice, data  Monitoring is an area that needs a lot of work
6	computer networking provides for access to application requirements. Every one of these applications is important both ashore and afloat.
7	As an application provider, I am most interested in remote application use.
8	Wireless will allow the implementation of monitoring sensors without the cost associated with installing cabling on ships - this is key!  RF id is key for security of PC assets on the ship in the future, we need to be able to tag our PC assets and track them on the ship.  Wireless is a cheaper way to get IP connected users on the ship, it is just that simple - they problem is we have not had a champion to spearhead this cause and this is costing all command big dollars due to duplicative efforts.
9	Remote Monitoring and Control is a must to ensure that networks remain secure. RF Identification is needed for asset and inventory control.
10	eoss ietms atfp personal locator damage control heat stress electronic logs
11	all play an equal role .... in supporting the warfighters needs
12	Voice and text msgs are an app that can revolutionize efficiency at sea since much time and energy is wasted on locating and speaking with other crew members. That's from a supervisory or co-worker coordination-collaboration standpoint. Second, inventory control and configuration need to be more efficient. Current practice is people intensive and prone to error. Remote monitoring can provide input to ship readiness and maintenance. This area should be more objective.
13	NTSR



## Appendix F, Day One Survey Results

14	Application developers will find innovative solutions to accommodate the mobile user, as we develop ways to secure wireless
15	Shipboard Warehouse Management System - T-AKE
16	n/a
17	Ranking of these areas is not relevant here. The discussion should be how to implement WLAN, it has been ID as a requirement, the application or purpose is not relevant until there is an infrastructure for the application.
18	Wireless connectivity can provide always on SA for commanders with the ability to communicate with watchstanders at any time.
19	Not partial to any area.
20	For the Navy, the big three are going to involve communications or monitoring plant processes.
21	The most important applications of wireless networks enable information access for warfighters in the field. This is the area where wireless networks will be a necessity not just a convenience or money saving device.

### 11. Capabilities. Allocate 100 points between the following categories to indicate their relative importance as capabilities of wireless networks.

(Allocate all resources.)

#### 2.13. Operational range—either to extend or to limit (meters/kilometers)

Low	High	Avg	Med.		#
1	30	7.78	10		47

#### 2.14. Speed of mobile communications (e.g. bandwidth v. speed)

Low	High	Avg	Med.		#
1	100	13.85	10		47

#### 2.15. Speed and ease of installation (time, simplicity)

Low	High	Avg	Med.		#
1	95	10.23	10		47

#### 2.16. Security/encryption (access control, information assurance)

Low	High	Avg	Med.		#
10	90	25.93	30		47

#### 2.17. Bandwidth/throughput (bits per second)

Low	High	Avg	Med.		#
1	50	17.02	15		47

## Appendix F, Day One Survey Results

### 2.18. Ruggedness (perform in adverse environments)

Low	High	Avg	Med.		#
5	70	10.19	9		47

### 2.19. Other

Low	High	Avg	Med.		#
40	40	0.85	0		47

### 2.20. Portability (size, weight, power requirements)

Low	High	Avg	Med.		#
1	80	14.12	10		47

## 12. Please explain your answer on capabilities. If you selected the "Other" category, please describe what category you had in mind.

(Click in the box to enter text.)

#	Comment
1	Developing secure wireless capabilities (making rational/evaluated risk management decisions) has to be the most important . I fear that as our dependency on this technology grows, so does our vulnerability
2	Regardless of the system that is put in place GIGO still applies, we need to safeguard the data at all levels to ensure we are working off ground truth and not something that has been redirected or manipulated.
3	Need security, ruggedness and speed to install as keys for operational utility. Other items contribute but are not as important.
4	Security is never easy and seems to sacrifice speed and size.
5	Security must be addressed but would like to see a single accreditation source
6	Wireless networking is important because:  1. it is low cost way to implement a shipboard network 2. mobile computing is needed now
7	Bandwidth and Security are key capabilities in ensuring that the end user can perform his or her job in a secure and reliable network. This includes the ability to manage bandwidth at the PC level.
8	If wireless networks cannot support secure encrypted operation they will be limited in their application and we will never be able to realize the goals of FORCEnet and the GIG.
9	Security, portability and ease of use are critical - most other aspects can be optimized through Training and CONOPS. Also the importance of KM PROCESS is what will enable the largest gains in wireless - applications/databases can be resident on local CPU with minimal BW requirements for the exchange. We don't NEED to pass mega PPTs over the WLAN - only the data changes.

## Appendix F, Day One Survey Results

10	Security is the number one issue needing resolution.
11	Mobility and portability are the crucial capabilities that wireless provides. Making them easy to use is essential to reaping the benefits of wireless.
12	I am viewing this from a T-AKE only viewpoint
13	n/a
14	Security appears to be the limiting factor, there is technology available but it needs to be tailored to operate in a Navy environment.
15	Wireless connectivity will allow the CSG/ESG commander to in essence bring his own bandwidth to the party. With wireless between the ships you will see higher throughput to the small decks with the big deck serving as the hub of the wheel.
16	I only wanted to emphasize bandwidth requirements and security concerns.
17	Other:  QOS and COS is extremely important, since this stems from a mandate named 'Assured Service'.
18	Security and range is more important than speed and portability at the moment is both are lacking in current implementations. (They're getting better though.)
19	security is the one importance/of the all the capabilities....once our level of security is meet all killer apps will follow.

### 13. Challenges to Delivering Wireless Networks. Allocate 100 points between the following categories to indicate their relative importance as challenges to delivering wireless networks.

(Allocate all resources.)

#### 2.21. Identifying user needs

Low	High	Avg	Med.		#
5	75	14.85	10		47

#### 2.22. Matching needs with capabilities

Low	High	Avg	Med.		#
5	40	10.7	10		47

#### 2.23. Meeting security requirements

Low	High	Avg	Med.		#
10	80	31.85	33		47

#### 2.24. Meeting policy requirements

Low	High	Avg	Med.		#
10	60	23.25	20		47

**2.25. Selecting and implementing the technology**

Low	High	Avg	Med.		#
10	50	8.8	10		47

**2.26. Justifying the value of wireless networks to achieve funding**

Low	High	Avg	Med.		#
5	50	10.1	10		47

**2.27. Other**

Low	High	Avg	Med.		#
20	20	0.42	0		47

**14. Please explain your answer to the above question on challenges to delivering wireless networks. If you selected "Other," please describe what category you had in mind.**

(Click in the box to enter text.)

#	Comment
1	The rate of change in the technology and the consistently shaky ground of policy not being official cause major headaches for taking technology out of the LAB... Sooner rather than later would like to get to implementation vice death by demo.
2	Have to overcome security and policy issues to get installation approvals, can't design system without knowing what user needs it has to provide capability to address, selecting and implementing technology essentially a network design problem but needs to be IAW user needs, security/policy issues. Justification should be based on comparison to wired, survivability, ability to reconfigure/reconstitute, technology refresh cost, i.e. life cycle aspects.
3	There are so many solutions and the issue is implementing a solution so it satisfies policy and security rgmts.
4	Once again, you have identified the key issues. If we can solve some of these then it will be easier to justify the value of WLAN to achieve funding.
5	Policy road blocks are difficult to resolve and have significantly held up the process of deploying these networks  Security solutions exist and must be agreed to and focused on to allow us to move forward.
6	Meeting both security requirements and policy requirements will slow down the "Speed to Capability" concept that the Navy has adopted.
7	Changing policy to allow implementation of wireless technology will be the most difficult task. In order to realize the real advantages of wireless networks DoD will need to change several policies and adopt a different view of warfighting.
8	review comments above

## Appendix F, Day One Survey Results

9	Security and policy are the major hurdles.
10	The most difficult aspect of WLAN fielding is justifying why we need it, wired LANs exist today and serve the purpose why should be expand into wireless?
11	A lot of fear currently exists as to the vulnerabilities associated with wireless technology. The best way to put to rest these fears is to understand the risk and vulnerability to these risks and design solution that manage the risks accordingly
12	Current accreditation process is difficult to understand. Lack of official guidance hampers deployment of wireless systems.
13	User Needs were our primary concern in developing SWMS. Now However, in order to implement we MUST get past security
14	Security requirements are #1 because we may have to have a WLAN to process classified data due to the aggregate data requiring classification.
15	Security and policy are the keys, solve these and the rest will fall into place.
16	IA is imperative when establishing the requirements for WLANs.
17	Once the appropriate technology is determined the other categories are all fixed.
18	How do we lock-in a technology today that will be obsolete tomorrow. How can we determine ROI for a system that has such a rapid technology refresh.
19	The main challenge is meeting all the requirements allocated by DoD regulations, such as the GSCR (Generic switching Communication Requirements) especially appendix 1, 2 and 3.  The Joint pub 6212 and 6215.
20	The hardest part about delivering 802.11x technology is having a legitimate justification for the technology. Most "requirements" amount to "convenience".
21	NSTR.

### 15. Test and Evaluation Venues. Allocate 100 points between the following categories to indicate their relative value as venues for wireless networking test and evaluation.

(Allocate all resources.)

#### 2.28. Scheduled ship and unit deployments

Low	High	Avg	Med.		#
5	100	32.22	30		45

#### 2.29. Training exercises

Low	High	Avg	Med.		#
10	80	27.51	30		45

#### 2.30. ACTDs (Advanced Concept Technology Demonstrations)

Low	High	Avg	Med.		#
5	70	13.53	10		45

**2.31. Specialized wireless network testing events**

Low	High	Avg	Med.		#
5	50	21.17	20		45

**2.32. Other**

Low	High	Avg	Med.		#
25	100	5.55	0		45

**16. Please explain your answer to the above question on test and evaluation venues. If you allocated points to "Other," please describe what category you had in mind.**

(Click in the box to enter text.)

#	Comment
1	joint operations/testing (other than actd) and sea trial like events
2	Actual shipboard testing is the only way to quantifiably produce data that supports implementation in the fleet, environmentals play a key role in RF propagation at sea and that can not be duplicated in the lab.
3	Felt they were all about the same
4	Demonstrations and testing are sacrificed for opn needs in turn sacrificing security.
5	It is time to stop avoiding the end goal, lets put the networks on ships and learn as we go. Start with NIPRNET and work toward SIPRNET.
6	Test and Evaluations should be performed in controlled environment such as the 'Sea Trail' process and ACTDs. Plus there are several ONR sponsored FNC's that would fit as well.
7	Warfighters need the opportunity to use and evaluate wireless solutions in operational environments in order to help specify the real requirements and most useful applications.
8	Quality testing needs to done in a at sea environment.
9	FORCEnet and the SBBL (USS CORONADO) are two key enablers that can provide optimal Wireless venues at minimal cost and impact to deploying fleet units.
10	All are important. As a COI a coordinated effort should be made to coordinate test and evaluation opportunities and share the information gained
11	Testing and evaluating wireless networks in their actual operating environment will provide the most accurate data.
12	I don't work in a T&E environment. We are installing a production system.
13	For new construction, test at yard and during trials.
14	Unless these are ACAT programs which I doubt then test during deployments and training exercises (spiral development).
15	Test wireless configurations in a test environment first and then fast track the selected ones to the fleet for implementation.
16	Not partial to any one area.

## Appendix F, Day One Survey Results

17	This technology moves too fast for normal acquisition processes. An ACTD will push procurement time frame by years.
18	Training and exercises are the probably the most important issues, as long as it is performed in a 'REAL ENVIRONMENT', since the feedback and valuable information can directly provide mission essential 'LESSON LEARNED'. Simulation and Modeling as well as Lab environment test and Evaluation...is exactly that....evaluation!
19	Lab tests cannot foresee the "environment" where ship and unit deployments can.
20	No comment.

### 17. Test and Evaluation Measures. Allocate 100 points between the following categories to indicate their relative importance as measures for wireless networking test and evaluation.

(Allocate all resources.)

#### 2.33. Performance--did it work as planned?

Low	High	Avg	Med.		#
10	100	22.23	20		46

#### 2.34. Effectiveness--as it useful?

Low	High	Avg	Med.		#
5	55	21.3	20		46

#### 2.35. Interoperability--did it work with other systems?

Low	High	Avg	Med.		#
5	50	18	20		46

#### 2.36. Information assurance--was its security adequate?

Low	High	Avg	Med.		#
10	100	23.13	20		46

#### 2.37. Cost savings--did it save money?

Low	High	Avg	Med.		#
5	90	14.02	10		46

#### 2.38. Other

Low	High	Avg	Med.		#
10	50	1.3	0		46

**18. Please explain your answer to the above question on test and evaluation measures. If you allocated points to "Other," please describe what category you had in mind.**

(Click in the box to enter text.)

#	Comment
1	All are equally important. Each contributes to the decision on how to proceed
2	Once the issues of detectability are resolved the chief concern that I have is whether or not we provided a useful tool to the fleet and a fair cost.
3	Should also test for how well it survives anticipated threats to robust operation and ability to perform from various types of attack against it.
4	every one wants more for less and the technology is not mature enough to meet the demand without sacrificing security
5	In order to acquire for any community, must be able to demonstrate cost savings
6	Did it save funds that is the bottom line.
7	Performance is based on the ability to perform the outlined test which is important. Also IA must be tested in accordance with existing policies.
8	Wireless networks can not be truly effective if they are not secure.
9	Security will always be a critical piece of Wireless. However, if you take that as a give - then the key metrics are INTEROPERABILITY with existing LAN and other applications and performance.
10	No comment.
11	Most important things at this stage are verifying security and effectiveness (which implies adequate performance). The rest can follow once these are known.
12	Compatibility - did it operate compatibly in the intended electromagnetic environment. Not causing interference and not suffering from interference. Further, will the ship be able to use it foreign ports and overseas ...i.e. Host Nation Coordination ?
13	n/a
14	These are the only two items the T&E will be judged on. Saving money is subjective, you can make the numbers say anything. As for security, if your not confident that it is secure then do NOT deploy.
15	Make it secure, make it work, make it meet the requirements.
16	Again, not partial to the categories.
17	Interoperability will ensure seamless communication across all services and agencies...a service entity cannot win a war alone!
18	Did it save money is usually asked first, followed by "did it work".
19	If its not useful, don't use it.
20	system needs to work 24/7.....



**19. Test and Evaluation Obstacles. Allocate 100 points between the following categories to indicate their relative importance as obstacles to test and evaluation.**

(Allocate all resources.)

**2.39. Lack of common test and evaluation objectives**

Low	High	Avg	Med.		#
10	100	22.7	20		44

**2.40. Lack of common test and evaluation measures**

Low	High	Avg	Med.		#
10	70	21.43	20		44

**2.41. Lack of test and evaluation opportunities**

Low	High	Avg	Med.		#
5	50	13.59	10		44

**2.42. Lack of cooperation from potential test organizations, units, ships, etc.**

Low	High	Avg	Med.		#
5	70	16.72	20		44

**2.43. Operational demands on organizations, ships, etc. that prevent complete test and evaluation**

Low	High	Avg	Med.		#
5	75	21	20		44

**2.44. Other obstacles**

Low	High	Avg	Med.		#
20	100	4.54	0		44

**20. Please explain your answer to the above question on obstacles to test and evaluation. If you selected "Other," please describe what category you had in mind.**

(Click in the box to enter text.)

#	Comment
1	Security is the obstacle
2	Felt they had equal weighting.
3	testing along with training are always sacrifice due to budget cuts. Standardized approach can minimize these costs
4	Funding resources required for T&E. It is difficult to get Fleet units many times but is worth the while if it can be done.
5	The challenge will be get a platform to devoted to a T & E process, you will probably have to link up to another test in progress

## Appendix F, Day One Survey Results

6	Both will cause a test report not to be accurate.
7	The new FRP process will limit our opportunities to test on fleet units.
8	sometime syscoms and operational cmd don't communicate well...
9	I am constantly surprised by the number of individual projects that are on-going doing testing that has already been accomplished in another test.
10	It is important to have a Navy coordinated test and evaluation initiative. There are many benefits to a managed process (i.e. shared lessons learned, avoid duplication of effort)
11	Many test criteria still not specified.
12	n/a
13	All are potential obstacles.
14	FRP ship skeds and higher authority will dictate the implementation of wireless in the Fleet.
15	Not partial.
16	A concise and clear objective that provides a mission essential requirement is extremely important, since a test and evaluation should be derived from Information Exchange Requirement (IER) from a specific entity
17	With newer technologies, there's often no accepted standard. Rather, each manufacturer will produce their own standard and hope that the rest of industry adopts it.
18	Funding. T&E can be expensive, especially if retesting is required.
19	NO comment/

### 21. Acquisition source. Allocate 100 points between the following categories to indicate the percentage of time that they will be the acquisition source for wireless networking technology over the next five years.

(Allocate all resources.)

#### 2.45. COTS (commercial-off-the-shelf)

Low	High	Avg	Med.		#
10	100	65.93	70		43

#### 2.46. GOTS (government-off-the-shelf)

Low	High	Avg	Med.		#
5	50	20.23	20		43

#### 2.47. Formal procurement

Low	High	Avg	Med.		#
5	80	13.83	10		43

#### 2.48. Other

Low	High	Avg	Med.		#
0	0	0	0		43

**22. Please explain your answer to the above question on acquisition sources. If you allocated points to "Other," please describe what category you had in mind.**

(Click in the box to enter text.)

#	Comment
1	Essentially application dependent.
2	I think that COTS is going to be the initial source but that GOTS will build off COTS technology.
3	I don't understand what you mean between Formal procurement and COTS and GOTS. All procurements are either GOTS or COTS or Mil specific. All procurements are done by a formal procurement or other contracting methods. You've mixed apples and oranges in this question. :-)
4	question unclear
5	Once specs are settled in area of security, commercial sector will respond with products. Other sectors, such as manufacturing will have many of the same requirements as the Navy.
6	Formal procurement, does not require a 'Title ten' or purchase during a War time situation.
7	I feel for financial reasons this proportion of spending is more cost effective.
8	Since formal procurement takes much longer than 5 years it gets a 0 here.
9	In the C4I area almost all commercial or a hybrid COTS and GOTS systems and products.
10	MSC ship, performance based acquisition approach
11	We need to follow industry as much as possible.
12	Navy has made a decision to go with COTS for cost.
13	This should be a strictly COTS venture, without modification.
14	With a product implementing Common criteria, that meets the needs of most.

**23. Wireless Information Classification: Assuming security requirements could be met, allocate 100 points between the following categories to indicate the percentage of wireless networking traffic that falls within these classification categories over the next five years.**

(Allocate all resources.)

**2.49. Unclassified**

Low	High	Avg	Med.		#
10	100	35.71	30		46

**2.50. Sensitive but not classified**

Low	High	Avg	Med.		#
10	80	26.28	25		46

## Appendix F, Day One Survey Results

### 2.51. FOUO (For Official Use Only)

Low	High	Avg	Med.		#
5	60	11.1	5		46

### 2.52. Confidential or Secret

Low	High	Avg	Med.		#
1	50	21.19	20		46

### 2.53. Higher than secret

Low	High	Avg	Med.		#
1	80	5.69	0		46

### 2.54. Other

Low	High	Avg	Med.		#
0	0	0	0		46

**24. Please explain your answer to the above question on network classification. If you allocated points to "Other," please describe what category you had in mind.**

(Click in the box to enter text.)

#	Comment
1	Few classified solutions exist
2	Unclassified related to RFID.
3	Most users only need a SABI solution
4	Most will be unclas or sensitive material including QOL applications. As security gets better, more will migrate to WLAN.
5	It will take sometime for DoD to get comfortable to with wireless operations, so NIPRNET will be the dominate user in the near-term.
6	Unclass is the only way to go.....Secret is to vulnerable
7	Need sources easier to maintain than say SECNET 11 for classified
8	As we move Command and Control data onto wireless networks secret data requirements will increase.
9	I think that the initial thrust will be UNCLAS but once technology is proven out other enclaves will follow suit.
10	Self explanatory.
11	It will be a mix. Exactly what mix remains to be seen -- it depends on the operational and business cases that can be made.
12	This is for the T-AKE SWMS System
13	This is the #1 issue for T-AKE WLAN. Not established yet whether the WLAN will be SBU or confidential. The aggregate data at the server is confidential. May be able to have a SBU WLAN with appropriate high assurance guards.

## Appendix F, Day One Survey Results

14	Id security is not resolved just UNCLASS, if that.
15	SA for the roaming commander will bring wireless to the SIPRnet.
16	I don't think unlicensed devices should be used for classified uses.
17	The suggestion in the Joint community, including the IRAK War, is that IP or Wireless will be done in a IP SIPRNET/DRSN environment. VPN might be the other venue for other classification traffic.
18	Unclassified is where all of the "entertainment" is.
19	I don't see anything other than unclassified being used for a while.

### 25. Select ANY of the following to indicate what roles you believe should be played by a wireless networks community of interest.

(Choose up to the maximum number of selections.)

	Count
<b>SHARE information on wireless network PROGRAMs and POLICIES</b>	<b>44</b>
<b>SHARE information on wireless network TECHNOLOGIES</b>	<b>42</b>
<b>COORDINATE wireless network activities</b>	<b>38</b>
<b>PROPOSE policies for other organizations to approve and implement</b>	<b>34</b>
<b>IMPLEMENT policies approved by other organizations</b>	<b>24</b>
<b>APPROVE policies</b>	<b>17</b>
<b>ENFORCE compliance with policies</b>	<b>21</b>
<b>Other</b>	<b>2</b>

### 26. Priority of effort by a wireless networks Community of Interest (COI). Allocate 100 points between the following categories to indicate the relative priority of effort of a wireless networks COI.

(Allocate all resources.)

#### 2.55. Sharing information

Low	High	Avg	Med.		#
10	100	40.59	40		47

#### 2.56. Coordinating activities

Low	High	Avg	Med.		#
10	50	26.78	30		47

#### 2.57. Proposing, implementing, or approving policies

Low	High	Avg	Med.		#
10	80	22.08	20		47

## Appendix F, Day One Survey Results

### 2.58. Enforcing policies

Low	High	Avg	Med.		#
5	40	7.87	0		47

### 2.59. Other

Low	High	Avg	Med.		#
25	100	2.65	0		47

**27. Please explain your answer on priority of effort. If you selected the "Other" category, please describe what category you had in mind.**

(Click in the box to enter text.)

#	Comment
1	Reducing and streamlining the approval process to allow implementation of WLANs.
2	Felt these were appropriate breakdowns.
3	I have found that most organizations share their work. Eventually, as I, you get to know the folks involve in this arena  Lack of enforcement of policy is a killer today!
4	All these functions are what I expect from this forum and group of SME's.
5	Lack of succinct policy and associated single point of reference is an issue
6	The COI should be a sharing/coordinating body!
7	You usually do not have the decision makers involved in these meetings.
8	Right now information on policy and wireless activities scattered.
9	I think that the COI should focus on information sharing so that efforts are not duplicated and taxpayer funds are optimized.
10	NTSR
11	Should not be involved in enforcing policies. Should advise that that enforce policies.
12	OTHER: Proposing and developing wireless LAN standards to be used across the COI and ensuring that the SYSCOMs and various wireless LAN acquisition agents incorporate a rigorous System's Engineering Process (risk management) for implementing and developing a wireless LAN capability.
13	n/a
14	abc should be 123, except for approving and enforcing policies, this body should propose and follow up with implementation support to PMs and other activities.
15	Coordination and sharing are needed to avoid duplication of effort.
16	Not partial.
17	This is relatively new, thus a group of this gender should provide proposal to CCB to implement and enforce policies.

## Appendix F, Day One Survey Results

18	Effective policies must be enforced to ensure security.
19	The COI needs to coordinate activities and share information. It is unlikely the COI will have strong influence on policies.

### 28. Potential wireless networks Community of Interest (COI) products. Allocate 100 points between the following products and services to indicate what the COI should produce.

(Allocate all resources.)

#### 2.60. Regularly scheduled meetings and conferences

Low	High	Avg	Med.		#
5	90	21.33	20		45

#### 2.61. Website, newsletter, or published reports

Low	High	Avg	Med.		#
5	80	20.55	20		45

#### 2.62. Technology demonstrations/industry days

Low	High	Avg	Med.		#
5	40	11.88	10		45

#### 2.63. Proposed policies

Low	High	Avg	Med.		#
5	60	17.22	20		45

#### 2.64. Proposed security standards

Low	High	Avg	Med.		#
5	75	14.33	15		45

#### 2.65. Proposed technical standards

Low	High	Avg	Med.		#
5	60	13.55	15		45

#### 2.66. Other

Low	High	Avg	Med.		#
50	50	1.11	0		45

**29. Please explain your answer on products. If you selected the "Other" category, please describe what category you had in mind.**

(Click in the box to enter text.)

#	Comment
1	All of the above.
2	A regular feedback to participating COI groups maintains visibility and effort active.
3	Serious security standards seems to important to allow on an unlicensed device.
4	Make the policies and get the information out there!
5	Need to concentrate on products otherwise just identify this as a coordinating body to discuss wireless.
6	n/a
7	It is imparitive that the process for approval of the various aspects be defined and streamlined immediately. The Navy is far behind industry today in this area. In a year the systems we are talking about today will be obsolete.
8	Contribute to the DoD Wireless Knowledge Management Process
9	Pull technology using either NKO or other web sites for information will allow others to gain information.
10	COI activities should be centered on coordination and information sharing.
11	Meetiings should be held for informational purposes and also reviews of standards and policies should be done.
12	COI should share and distribute what is applicable to wireless activities
13	This should be more of a policy and deliberation group, although a sharing information vehicle is highly desired.
14	With a good security and technical standard, policy almost falls out. Some sharing/gathering build relationships and the reality is work is about relationships
15	Policy and website to get information seem to be more important at first cut.

**30. Priority of Issues. Allocate 100 points between the following categories to indicate your proposed priority of effort for addressing wireless networks issues.**

(Allocate all resources.)

**2.67. Operational requirements issues**

Low	High	Avg	Med.		#
10	60	21.73	20		45

**2.68. Policy issues**

Low	High	Avg	Med.		#
10	70	24.4	20		45



## Appendix F, Day One Survey Results

### 2.69. Information assurance

Low	High	Avg	Med.		#
10	80	26.55	25		45

### 2.70. Technical issues

Low	High	Avg	Med.		#
1	50	13.91	10		45

### 2.71. Implementation and acquisition issues

Low	High	Avg	Med.		#
5	40	13.4	10		45

### 2.72. Other

Low	High	Avg	Med.		#
0	0	0	0		45

## 31. Please explain your answer on priority of issues. If you allocated points to "Other" categories, please describe what categories you had in mind.

(Click in the box to enter text.)

#	Comment
1	No comments.
2	Operational requirements need to drive the implementation of WLAN, if there are none then we shouldn't do it.
3	Seems from what was presented today that all the other areas are/were being really worked but the acquisition issues on how to get this technology out and into the fleet operationally was lagging.
4	SO many products to select from and to decide what is the best configuration to address security, flexible enough to stay on top of technology, and meets everyone needs
5	Each of these is important to the overall effort to achieve wireless LAN's.
6	We need to come through the policy roadblocks and get these networks in the fleet - that is where we will learn their true value.
7	question unclear
8	Information assurance issues are unique to the military so most DoD time should be spent solving those issues.
9	The technology is there for anything you want to do. It is the details -- security, EMCONN, authentication -- that are crucial.
10	n/a
11	All are important, some are not as far along, for example THIRDFLT stated it's requirements but IA policy is playing catch up to the technology.
12	Set the security policy, meet the Fleet requirements, and acquire it.

## Appendix F, Day One Survey Results

13	Not Partial.
14	The operational issue is a killer or a money category, if a C2 requirement is injected into the wireless effort, much support will be provided....any other issues is just semantics.
15	Accreditation is usually the hard part of the job.
16	Operational Requirements will drive everything

### 32. Day One Assessment. Using a scale of 1 to 10 indicate your assessment of Day One. [1=waste of time, 5=valuable event, 10=exceptionally valuable event]

(Rate from 1 to 10, with 10 the highest value.)

1	2	3	4	5	6	7	8	9	10	Total
0	0	0	1	3	3	9	15	9	7	47

### 33. General comments on Day One. Please offer any comments you have regarding Day One and any suggestions on how to improve the Wireless Networks Summit.

(Click in the box to enter text.)

#	Comment
1	No technical data supporting EMI IA issues. Currently at the bleeding edge so studies and reports not available.
2	One or two survey questions were confusing Survey was too long
3	1. good facility, food layout was afterthought in the layout of the facility. 2. More case studies would be helpful, less intro back and forth with briefers. 3. software really needs be next generation. it is basically chat room software. need tree view sorted by comment #. current system is moderately useful.
4	Great Meeting - I hope to see major changes by next meeting DUE TO PUBLISHED STANDARDS for General NAVAL implementation of NIPR/SIPR Wireless LAN augmentation architecture.
5	Well organized and informative.
6	I thought that the agenda for the day was well put together, the case studies were an excellent way to show the issues, commonality of the issues across platforms, and were the potential hurdles are in implementing wireless technology afloat.
7	none right now
8	Nicely done. Advance expectation was that more of the PDA / PED issues would be addressed, but this is a nice facility and some very good presentations. Thank You.
9	I hope this cause NETWARCOM to assume the role of Wireless Coordinator!
10	none
11	The first day has been interesting and useful. The collaboration software enables sidebars without taking people out of the main group.
12	na
13	great summit

## Appendix F, Day One Survey Results

14	great job of packing a lot of information into a short time frame... all presenters did a good job of setting the tone for where we are today... free flowing groupware comments added a lot of valuable information looking forward to the rest of the summit
15	Enjoyed. Learned a lot.
16	Case studies were very helpful in defining our way forward.
17	I think the Groupware concept is an excellent way to solicit inputs from the entire community. Great forum.
18	Excellent Material. I take it the briefs will be made available to the attendees as there wasn't enough time in all cases to digest everything on the briefs.
19	Good first try, brought out a lot of issues.
20	Fast moving and interesting. The chat room added considerable value and aided in speeding along the discussions.
21	Really enjoyed the first day.
22	The information I gathered today will serve as another valuable asset to my Program Managers. I can use and assess some of the scenarios in my lab and determine how a JOINT environment can affect the Warfighter and improve prior to the annual Joint User Interoperability Communication Exercise (JUICE 04).
23	Do away with the observer group? I started in that group and it was a bit boring.
24	Add some type of Internet access or kiosk. Provide read aheads that include an overview of wireless concepts and terms. Distribute an acronym list.
25	good recap of current situation, however a bit redundant for those who have been in the community. Probably could have GONE WITH 2 Case studies and a summary of a few others to leave more room in the agenda for planning the road ahead. Also, need to define an executive steering group for this body that is chartered with the decision making and the road ahead - Looks like many of the people near the center of the circle of the seating.
26	Explain a bit more on the groupware to squash some of the commentary about it. Try to....
27	NSTR.

## Appendix F, Day One Survey Results

Intentionally Left Blank

## APPENDIX G

### Summary Survey Results Wireless Networks Summit

**1. Select one of the following categories that best describes your professional experience.**

(Choose one.)

	Count
<b>Engineering/technical</b>	<b>14</b>
<b>Research and development</b>	<b>7</b>
<b>Acquisition</b>	<b>6</b>
<b>Analysis</b>	<b>1</b>
<b>Communications / computers</b>	<b>9</b>
<b>Intelligence</b>	<b>0</b>
<b>Operations</b>	<b>3</b>
<b>Training and doctrine</b>	<b>0</b>
<b>Other</b>	<b>1</b>

**2. Select ANY of the following categories to indicate your objectives for attending this event**

(Choose up to 10.)

	Count
<b>Learn more about the Navy's approach to wireless networking</b>	<b>28</b>
<b>Learn more about wireless networking CAPABILITIES and APPLICATIONS</b>	<b>24</b>
<b>Learn more about wireless networking TECHNOLOGIES</b>	<b>27</b>
<b>Learn more about wireless networking POLICY and SECURITY ISSUES</b>	<b>30</b>
<b>Learn more about the wireless networking Community of Interest (COI)</b>	<b>21</b>
<b>Join the wireless networking COI</b>	<b>17</b>
<b>Influence the selection of wireless networking TECHNOLOGIES</b>	<b>19</b>
<b>Influence the resolution of wireless networking POLICY and SECURITY ISSUES</b>	<b>21</b>
<b>Influence the Navy's approach to wireless networking</b>	<b>21</b>
<b>Other</b>	<b>2</b>

**3. Select one of the following categories to describe yourself**

(Choose one.)

	Count
<b>Active duty military</b>	<b>10</b>
<b>Civil servant</b>	<b>22</b>
<b>FFRDC/UARC employee</b>	<b>0</b>
<b>Government contractor employee</b>	<b>8</b>
<b>Industry/commercial employee</b>	<b>1</b>
<b>University or academic employee</b>	<b>0</b>
<b>Other</b>	<b>0</b>

**4. Select one of the following categories to describe your relationship to wireless networking**

(Choose one.)

	Count
<b>Current program manager (manage/support manager of a current wireless program)</b>	<b>14</b>
<b>Current user (use of a wireless network)</b>	<b>1</b>
<b>Current stakeholder (have a vested interest in a current wireless network)</b>	<b>6</b>
<b>Current implementer or acquirer</b>	<b>6</b>
<b>Potential program manager</b>	<b>0</b>
<b>Potential user</b>	<b>1</b>
<b>Potential stakeholder</b>	<b>2</b>
<b>Potential implementer or acquirer</b>	<b>5</b>
<b>Policy maker</b>	<b>3</b>
<b>Other</b>	<b>3</b>

**5. Industry Day. Using a scale of 1 to 10 indicate your overall assessment of Industry Day. [1=waste of time, 5=valuable event, 10=exceptionally valuable event]**

(Rate from 1 to 10, with 10 the highest value.)

1	2	3	4	5	6	7	8	9	10	Total
0	0	0	0	3	2	11	7	11	3	37

**6. Select ANY of the following choices to indicate ways to improve Industry Day.**

(Choose up to the maximum number of selections.)

	Count
<b>Allocate MORE time to Industry Day</b>	<b>3</b>
<b>Allocate LESS time to Industry Day</b>	<b>1</b>
<b>MORE exhibits</b>	<b>18</b>

## Appendix G, Summary Survey Results

<b>FEWER exhibits</b>	<b>0</b>
<b>MORE plenary / vendor presentations</b>	<b>11</b>
<b>FEWER plenary / vendor presentations</b>	<b>1</b>
<b>Broader focus of exhibits</b>	<b>7</b>
<b>Narrower focus of exhibits</b>	<b>2</b>
<b>Other</b>	<b>5</b>
<b>It was perfect. Do not change anything. [NOTE: please do not make any other selections]</b>	<b>9</b>

### 7. Please explain your assessment of Industry Day. How would you improve it?

(Click in the box to enter text.)

#	Comment
1	This was the most valuable portion of the program...my project is shopping for technology to solve the security issue right now.
2	Was unable to attend due to other commitments.
3	Need to ensure that current tech industry partners have a chance to collaborate with each other. Introduced several folks to each other so they could leverage their products with various other initiatives.
4	Realizing that vendors come on their own nickel it would still be nice to have a broader industry representation with time allocated for vendors to brief their vision.
5	Have some descriptive information in the Agenda book on each vendor's products and if they were going to have a separate briefing in one of the breakout rooms what the general focus of their brief was going to be. Also have sufficient breakout sessions setup so that same material could be replicated 2X or 3X over the breakout periods enabling attendees to cover more vendor breakout sessions when there were time conflicts during a breakout period.
6	30 minute allocation for each vendor was not enough time. At least 45 - 60 minutes
7	Add summary of technologies provided by the companies. Can then focus on which ones to visit.
8	Good mix of plenary & exhibit time
9	Need a broader view of the wireless industry and it would be useful to have someone from industry and government who has implemented wireless discuss their experience and lessons learned.
10	Industry day was a perfect opportunity to express our desires for specific products.
11	change arrangement of classroom gov't only briefings... on as needed basis.
12	more big boys like Motorola, Nextel and hp
13	Some very great presenters. I learned about some very useful products that I plan on recommending to superiors in order to support published policies.

## Appendix G, Summary Survey Results

14	The OSD talk was the highlight of the day because it gave the DoD vision for the future. It would have been nice to have one talk that gives industry's collective vision of where things are going in the commercial market. While they will not reveal proprietary data, I am sure there is broad agreement on trends.
15	Excellent, but would open to more vendors
16	get broader participation especially from what's is the next generation
17	Lance: Plan a little better - get vendor info out ahead of time, get speakers lined up earlier.
18	need more time for the vendor briefs
19	I would like to see more vendor exhibits and more hands on presentations.
20	None of the big guys where here (Boeing, Lockheed Martin, etc.)
21	Provide a list of topics that the vendors will present. I selected presentations based solely on vendor name.
22	It is just right.
23	Industry day was very useful.
24	Industry Day was very well organized and provided good information. Would have been better for vendors if more attendance in classroom sessions, but that was explained to them in advance.
25	There was a lot of down time. Not enough vendors to take up the time. Needed more participation in the vendor presentations.  Suggestion: Do one or the other between vendor booths or vendor presentations.
26	Possibly having specific topics/requirements and have vendors brief to those topics

### 8. Roadmapping Description and Discussion. Using a scale of 1 to 10 indicate your overall assessment of this activity. [1=waste of time, 5=valuable event, 10=exceptionally valuable event]

(Rate from 1 to 10, with 10 the highest value.)

1	2	3	4	5	6	7	8	9	10	Total
0	4	1	6	5	10	6	4	4	1	41

### 9. Please explain your answer to the above question. Please offer any suggestions on how to improve the process.

(Click in the box to enter text.)

#	Comment
1	If we had the data in this tool, We still need to create our plan (refined roadmap) for which we plan to follow identifying critical paths, plans of action, tasks, etc...
2	Didn't seem to have any useful product yet.



## Appendix G, Summary Survey Results

3	good concept, poor execution, if we are buying this service why are we adding and discussing future enhancements? much more up front discussion needs to be had before these surveys are conducted via email. Phone call prior and who gets to take the survey is critical otherwise garbage in and out
4	I looks like a fair method - did not see anything exciting or earth shattering....
5	We missed opportunities to clearly show how the tool can be used to influence when and where we conduct tests and when we can use existing data to satisfy a test or regulatory requirement.
6	Basic idea is good. As presented I found the graphics a little bit difficult to interpret. My organization is currently engaged in large scale RM of technologies and it is not an automated process so keeping the charts and data up to date will be a challenge. Found it hard to see some of the strategic aspects given the charts that were presented. Also how are disruptive technologies factored into the RM process?
7	The fact that the synergy tool had lack of response was not useful. I expected more from eTrust other than a description. I'd of thought a plug for us to start this process would have been initiated
8	This did not really provide any useful info (sorry). One of the comments on the "chat" groupware was that it seemed to be an overblown POA/M...
9	Roadmapping is a viable method of documenting direction but challenging to get appropriate stakeholder participation
10	I would like to see their suggestions/recommendations for wireless guidance
11	Would to have send a project/program mapped against the state of tech currently
12	The roadmapping discussion was focused on the tool and should have been focused on the roadmap.
13	survey limitations left bad taste in my mouth
14	more data would be helpful. tutorial on how the surveys work... use software live as opposed to canned presentation
15	The roadmap is very useful but the interview process must be improved. Being able to see everything that everyone else is doing is great.
16	The project didn't appear to be much more than a MS Project setup...if that. Although I agree with the use of these types of tools to wrap our brains around the problem and get things solved.
17	Roadmapping intro not needed. The roadmapping seems to be a compilation of POA&M's. Thought this group would discuss and attempt to lay out the way ahead, not just compile previous work.
18	Very similar to POAM process, which can also be done in a collaborative process, however it may not be NMCI...
19	Didn't discuss developing a roadmap just collecting data.
20	Need to do a better job explaining use and purpose of tool. A lot of negative comments about not seeing the value.

## Appendix G, Summary Survey Results

21	I like the structure and discipline roadmapping provides and think the tool was a good process/thought starter.
22	A lot of talk about how to do a roadmap, what cool tool we should use, but no real work on a roadmap.
23	The effort is only one of many other possibilities.
24	I like the concept of roadmapping but don't think it is worthwhile until all of us have access to the software.
25	Where else does one get the strategy and the meat behind it in DoD? One can guess by looking through the PreBud.
26	I think this will be an excellent tool if all WLAN COI uses it. It is a tool that can, if used correctly, focus this group of different organizations and schools of thought.
27	For those involved in roadmapping this was a useful session.

### 10. Select ANY of the following objectives that you think you accomplished during this event

(Choose up to the maximum number of selections.)

	Count
<b>Learned more about the Navy's approach to wireless networking</b>	<b>31</b>
<b>Learned more about wireless networking CAPABILITIES and APPLICATIONS</b>	<b>26</b>
<b>Learned more about wireless networking TECHNOLOGIES</b>	<b>26</b>
<b>Learned more about wireless networking POLICY and SECURITY ISSUES</b>	<b>35</b>
<b>Learned more about the wireless networking Community of Interest (COI)</b>	<b>27</b>
<b>Joined the wireless networking COI</b>	<b>15</b>
<b>Influenced the selection of wireless networking TECHNOLOGIES</b>	<b>2</b>
<b>Influenced the resolution of wireless networking POLICY and SECURITY ISSUES</b>	<b>7</b>
<b>Influenced the Navy's approach to wireless networking</b>	<b>9</b>
<b>Other</b>	<b>1</b>

### 11. Overall Assessment. Using a scale of 1 to 10 indicate your overall assessment of this event. [1=waste of time, 5=valuable event, 10=exceptionally valuable event]

(Rate from 1 to 10, with 10 the highest value.)

1	2	3	4	5	6	7	8	9	10	Total
0	0	0	0	2	3	5	21	9	1	41

## Appendix G, Summary Survey Results

### 12. Future Attendance. Using a scale of 1 to 10, indicate your desire to attend similar events in the future. [ 1 = No desire to attend, 5 = Moderate desire to attend, 10 = I insist on being invited]

(Rate from 1 to 10, with 10 the highest value.)

1	2	3	4	5	6	7	8	9	10	Total
0	0	1	0	1	3	4	13	6	13	41

### 13. Comments on assessment and future attendance. Please comment on your answers to the above questions on overall assessment and future attendance.

(Click in the box to enter text.)

#	Comment
1	I'd like to see a conference set up with a specific agenda to address policy and get current policies either up-to-date or out of draft. Let's shake this monkey out of the tree...
2	One of many commitments. We need to focus on concrete progress. We spent too much time on fluffy stuff
3	some duplication of briefs and information - was good for this initial meeting to bring everyone up to the same level. May want to break out into specific sessions next time: Security / Policy / Technology and T&E for working groups that report out at the end....
4	This is a great forum for openly discussing issues at an action officer level. decision level discussions are not generally held with the level of personnel that were in attendance. To solve hard policy issues, as I assume some thought we would, requires the participation of three and four star officers and equivalent civilian leaders.
5	Thought the event was well organized, material was for the most part on target for my needs, still have some confusion on way ahead for some areas, but looking forward to continuing to stay involved to eventually get the technology afloat.
6	Glad to see security is one of the highly valued concerns
7	My expectations were for more of an OAG type of event where we actually could put forth a way-ahead and possibly decide some actions. Maybe in future sessions. Still a valuable networking and "baselining" event where info was shared.
8	This was a good exchange of information but there needs to be clear objectives for the next one to justify this level of personnel participation
9	need panel of sme's at end of future summit  need usna and npgs to brief wireless network initiatives  need don cio himself as keynote speaker
10	Was hoping to get further on defining wireless requirements and identifying technical unknowns then assign tasks and actions. Then when the information is available it will be used to create/update/change the policies.

## Appendix G, Summary Survey Results

11	For this event of the last three days to have been worthwhile, there must be follow-up and there must be a roadmap that everyone can use. A follow up event and commitment to the roadmap must be outcomes of this meeting.
12	Annual events seem sufficient vice bi-annual.
13	When will minutes be published? Is NETWARCOM the DAA and where is the letter or charter for that ?
14	Need to assign actions. For example, create a warless technology roadmap to have something to discuss at a next meeting.
15	I think the event went very well. Need to respond to comments when planning the next one. I'll certainly be there.
16	I am from the NMCI project and would like to ensure our activities are linked with the Afloats policy and direction. I need to stay engaged with Wireless policy for our delivery and connectivity issues for ships.
17	Great networking opportunity.
18	I will be looking forward attending future summits, information gathered will improve my Command.
19	I am looking forward to the next summit to see how these discussions have evolved since this summit. Thought this was an excellent beginning.
20	The conference was useful but I don't think we got to the point of influencing any aspect of wireless implementation in the Navy. The information provided was useful. Further summits should be held to continue addressing the pertinent issues.

### 14. Future wireless networking activities. Select one of the categories below to characterize your recommendation for future wireless networking activities.

(Choose one.)

	Count
<b>Stop them, they have little or no value</b>	<b>0</b>
<b>Stop them, we have what we need</b>	<b>0</b>
<b>Continue them and keep the same basic design</b>	<b>20</b>
<b>Continue them but change the design</b>	<b>17</b>
<b>Don't know</b>	<b>1</b>
<b>Other</b>	<b>3</b>

### 15. Please explain your answer to the above question. If you selected "Other," please describe what you had in mind.

(Click in the box to enter text.)

#	Comment
1	Continue them, but have an enterprise coordinated plan (DoN, DoD, Joint) to optimize efforts
2	Some portions of the designs are fine. Some portions need further analysis and possible design changes, in particular the key technical issue of multiple WLANs on one ship.

## Appendix G, Summary Survey Results

3	We did a lot of issue identification this time. Next time we need to Include more time to on issue resolution.
4	I believe that open forum discussions are useful knowledge sharing ventures that need to continue until we reach a point that we do not have the authority to act, at which point the senior management needs to become involved.
5	It's an iterative process, too early to tell if any radical changes are needed. I would keep the same format for one or two more future gatherings then make changes at that point. Could be useful to subgroup into some functional areas - security, policy, acquisition, T&E etc. at some points in the gathering. A glossary of acronyms and other terms would also be useful in the handouts.
6	Start small and build upon them for technology is changing to rapidly at the cost of never ever getting anywhere if you tried to continually change your approach
7	The composition will change naturally....good indication that we are succeeding in transitioning the capability.
8	Break into group topics - interest items to include process to execution. Also, Naval process to get through an install.
9	Need to have policy to have a consistent approach with interoperability and supportability ashore and afloat
10	All the policy is in draft. It makes it hard for a new program to see how to proceed unless they are already a part of this group
11	Continue the summits but make them more of working group sessions with policy review, and decision making briefs.
12	see 13
13	like the format and the setting... would change some of the content and discussion topics.
14	Next time, we need to see more data in the roadmap and see how it can be used.
15	Continue wireless activities using reasonable defense and security applications. Write and enforce reasonable policies on the justified use of wireless networks and enabling technologies.
16	Recommend having NETWARCOM or other appropriate reps take the lead in leading discussion vice an independent moderator (although the moderator here did his job well). To attempt to gain more focus vice random discussion.
17	would recommend broader audience. Could give impression of stove pipe; impact of Telemedicine on bandwidth ? Some forms being used for triage already.
18	The meeting format is fine just need products.
19	Need higher level decision makers here.
20	Format is ok, but need less briefing next time (overview only in the areas that were briefed), and use more time to discuss issues to assist with the policy making and to consolidate/coordinate the efforts across the Stakeholders.
21	The approach is open for improvement and learning from other inputs or participants.
22	I would recommend spending more time developing products like policy recommendations etc.

## Appendix G, Summary Survey Results

23	Encourage a reasonable security policy, clarify that policy and design/redesign wireless networks based on that input.
24	I thought JHU APL was a great forum to host a meeting like this. With all the different organizations represented, Groupware really allowed people to voice their opinions without holding up the meetings. Great place to hold a meeting with people from different backgrounds.
25	Wireless vs. Wired ? Where is the list of requirements that support an wireless effort. Does wireless save money, manpower? We need to start document these items to influence the POM process.

### 16. Value of the Surveys. Using a scale of 1 to 10 indicate your overall assessment of the surveys. [1=waste of time, 5=valuable, 10=exceptionally valuable]

(Rate from 1 to 10, with 10 the highest value.)

1	2	3	4	5	6	7	8	9	10	Total
0	0	0	3	3	3	12	10	9	0	40

### 17. General comments on the Wireless Networks Summit. Please offer any comments you have regarding the design and conduct of this particular event.

(Click in the box to enter text.)

#	Comment
1	Learned a lot about the very significant issue of getting security and other approvals. Need the reference documents to be approved and posted where they can be accessed. Unless they are signed out it is difficult to make a case to spend money to implement.
2	One of many commitments. We need to focus on concrete progress. We spent too much time on fluffy stuff.  Without resource sponsor attendance, we are groping around on why our POM issues have been rejected. We must get the N6 resource sponsor(s) to attend.
3	more case studies, less overviews. roadmapping & surveys need to be rethought? did not go over well. and the companies should never pitch future enhancements? sales job? industry day good idea
4	I think that we should have had a handout of the briefs prior to the conference - it would have been nice to take notes during the discussion on the actual referenced slides.
5	Given the population base for the surveys they are of limited value with regard to policy related issues. A much broader and more senior population of respondents would be needed.
6	Very good event. My thanks and appreciation to all who organized, staffed and pulled together to make the event so productive and good time investment. BZ!
7	Very impressed with the Groupware! Now await the end result, collection of information

## Appendix G, Summary Survey Results

8	Summit is valuable forum for the identification of the issues and the development of viable strategies to address these issues, while reducing redundancy and optimizing the overall Naval investment. Good mix of community reps.
9	Good summit. I think more structured format for briefings. Need more in-depth on how to get through the processes - who are the POC's? What docs are available, what do we need to get resolved. More action item oriented. Agree with this statement.
10	We need to make sure this forum isn't a single blip on the radar
11	Wireless summits need to result in actions being assigned, plans being made etc.
12	very good as an initial event... looking forward to future collaboration to make the next one even better.
13	bz
14	Great forum...beef up the agenda.
15	Extremely useful. I did learn more about the technology, about the projects underway, and about what it will take to move everyone forward.
16	Well organized. For future events, develop more specific goals and focus on the primary goals (e.g. develop strategy to influence security/IA issues for WLANs).
17	would like to see what is just over the horizon, not sure that was addressed.
18	The event was very professionally run.
19	I was a great first effort. Despite many stumbles along the way I think it went extremely well.
20	I think the summit was extremely informative and a good exchange. I would like to have seen a more definitive direction on Policy and hope future meeting or COI activities stay on task for this.
21	Good start to networking and collaboration. It must be kept up after the event.
22	Great forum to get an idea of what is being worked in the field.
23	All services should have a similar summit, in fact the NAVY can actually lead all services and establish a JOINT or Coalition Summit, once the initial grounds are established.
24	I would recommend starting on Tuesday, that way Monday is a travel day. Include more users
25	Agenda was well planned and sectioned
26	Very well organized. Be sure to leverage off of other organizations to ensure you're getting a large scope of information..
27	See other comments
28	Would hope that the info data from the discussions with this collaboration 'chat' tool is cataloged and shared

**18. Comments on the Warfare Analysis Laboratory. Please offer any comments you have regarding the WAL facility, administration, and staff. What did you like? What needs improvement?**

(Click in the box to enter text.)

#	Comment
1	Facilities fine. In the future, recommend that the food/non-food costs of the conference fee be determined due to recent Navy rules for folks on local travel (only get reimbursed for non-food costs).
2	Friendly and helpful
3	WAL nice facility... software tool needs some serious work for this level of funding and facilities
4	Fantastic facility & Wonderful staff.... Meals/fee rather steep!
5	As always, I am impressed with the facility and the manner in which the staff interacts with the clientele. Thanks for having us and assisting in moving us along the road.
6	Excellent facility, great staff - wish I had similar facility in my organization. Also great way to capture the course of the meeting and to gather diversity of thoughts on the issues under consideration.
7	Very impressed with it! Certainly something I would suggest my office to leverage , aside from the SE contract
8	Superb facility and staff.
9	Great facility and staff. No improvement necessary. Perhaps security clearances and badges could be streamlined a little.
10	This is a tremendous facility and appreciate the hospitality
11	Outstanding Job.
12	This is a nice facility. The moderator was good and the facility was comfortable.
13	excellent facility and staff... very nicely done and professional in approach.
14	well executed and valuable
15	Wish we had a set up like this back home...fantastic!
16	I want to know how I can get one for myself! The facility is wonderful.
17	outstanding facility. How would we go about renting this for other communities of interest ?
18	Great facilities, the SW was a good means of communicating ideas.
19	Did a great job.
20	I am extremely impressed with both the facility and the staff. Everything was top shelf. I think the delivery media was very well delivered. All of the support staff were great.
21	Great venue and moderator.
22	Very good facility for meetings/summits.
23	Thanks for hosting this event. The facility is outstanding. Would love to tour the APL facility sometime.



## Appendix G, Summary Survey Results

24	The security access paperwork/documentation needs to be expedited to avoid 'escort badges'.
25	Great setup and admin. Staff was very courteous and well organized.
26	Wonderful facility to hold such an event with all of these different disciplines and agencies in the same room.
27	<p>Wonderful staff to work with.. John Nolen was an excellent moderator. Facility was great to have for bringing everyone together. Groupware was an excellent tool to use. Keep out of the hands of jokers like Tim Schuler and you'll be ok.</p> <p>Only complaint was not enough lunch on Industry Day - lots of greedy people - mostly men.</p>
28	See comment from #15
29	Great facility! Wish we had work spaces like this!

Intentionally Left Black

## APPENDIX H

### GroupWare Comments Wireless Networks Summit, 8-10 December 2003

Main comments (those not referring to other comments) are sorted by comment number.  
Referring comments (those referring to other comments) are listed beneath the comment to which they refer.

<b>1</b>	<b>GROUPWARE INTRODUCTION.....</b>	<b>1</b>
<b>2</b>	<b>OVERVIEW.....</b>	<b>3</b>
<b>3</b>	<b>DOD POLICY .....</b>	<b>10</b>
<b>4</b>	<b>ISSUES DISCUSSION .....</b>	<b>13</b>
<b>5</b>	<b>METHODOLOGY .....</b>	<b>23</b>
<b>6</b>	<b>CASE STUDIES.....</b>	<b>23</b>
<b>7</b>	<b>DAY 1 AND 2 RECAP .....</b>	<b>38</b>
<b>8</b>	<b>APPLICATIONS AND CAPABILITIES.....</b>	<b>43</b>
<b>9</b>	<b>TECHNOLOGY TRANSFER.....</b>	<b>50</b>
<b>10</b>	<b>TEST AND EVALUATION.....</b>	<b>58</b>
<b>11</b>	<b>ROADMAPPING.....</b>	<b>62</b>
<b>12</b>	<b>SUMMARY DISCUSSION.....</b>	<b>66</b>

### GroupWare Introduction

Please answer the question: “What are the chief benefits of wireless networks?”

MainC mt#	Ref: Cmt #	Comment
3		Mobility
4		Mobility
5		mobility
6		Mobility
7		cost
8		weigh reduction
	31	re #8: weight
9		Reduced infrastructure
10		easy network growth
11		portability

## Appendix H, GroupWare Comments

12		Improve mobility
13		Mobility, flexibility, cost & time savings
14		reduced manning
	41	re:14 how do you see wireless effort reduced manning at sea?
	42	re: 41 - example - navy smart stores program which provides for a total asset visibility with reduced sailor intervention in the tracking (using rfid, etc), strike down, on-board management and ordering of stores. total asset visibility also strengthens sea basing by expanding availability and visibility of stores, munitions etc across the BG
	44	re 42, while this reduces effort, does it specifically lead to reduced shipboard manning, or just free up the sailors to do other things?
	45	re:14 right now we have several stove pipe systems on the ships. ICAS, ACD, ISMS, FODMS, ISNS, VDDS. Even with these systems, when the alarm goes off in ...you name the space or equipment... the decision maker in CCS, CSMC, Bridge, CIC has to send a sailor to investigate. Wireless can provide cost effective solutions to this. Remote sensors, cameras, monitors...being able to see the problem where you are and making decisions based on what you see/know, not on what information is being fed second hand.
	47	re 44: short term- primarily the latter, but a real potential in manning reduction for, say, cvn 21 where we have the ability to fully integrate the process
	48	re 45: Also, with wireless PDAs you could have reconfigurable fly-away repair teams instead of the current static repair lockers. The DCA could wirelessly tell repair members where to go and choose the closest members to fight the fire/damage. This would allow for a reduced manning requirement for damage control.
	50	re 45: I think we have to be careful about reduced manning, although remote sensors are good, in many cases an experienced Sailor may be able to give you a more accurate assessment of the problem also fixing damage requires muscle power
	55	re 48, does this imply that the Navy has a specific number of personnel that will be assigned to damage control? What if the wireless network has to be turned off for EMCON requirements, how will the DCA cope? In a damage control situation will wireless actually reduce manpower requirements? In the recent historical cases, COLE, ROBERTS etc would wireless have helped?
	62	re:44 Your thoughts are correct in that manning reduction is complex and needs to address much more than simply workload reduction... WLAN technology in and of itself does not take a body off the ship but as an enabling technology coupled and leveraged with proven applications and policy changes can then be sent through NAVMAC for reduction analysis... This effort is to help align those application/infrastructure requirements.

## Appendix H, GroupWare Comments

	69	re: 55 the navy does have a very specific policy for damage control manning. The shipboard WLAN EMCON has been addressed and provisions are in place to control this. I don't see how wireless will help damage control manning but enhance the information flow. Imagine being able to sit in CCS as the CHENG or DCA and be able to see in real-time what the attack team can see.
15		cost, and
16		Convenience.
17		Improve strikeup with IT
18		reconfigurability
19		cost savings
20		mobility, flexibility
21		Installation cost savings, mobility, and flexibility.
22		Cost and Efficiency
23		Connectivity, mobility, interoperability
24		cost
25		savings in time, energy and funds
26		mobility and cost
27		The portability, anywhere access and lack of infrastructure
28		Reduced weight, reconfigurability, survivability, quick to reconstitute
29		avoided wiring costs, and an infrastructure for wireless applications
30		forktruck mobility
32		Increased asset viz
33		reduced shipboard manning and improved effectiveness
34		total asset visibility
35		mobility, increased productivity, cost
36		No Wires
37		untether the operators and maint techs
38		TEST

## Overview

MainC mt#	Ref: Cmt #	Comment
39		Dave Bartlett 9:37AM Monday
40		Emission detection & Security
43		can we get elec copies of the briefs before we leave Wednesday?
46		Vince Piarulli Wireless Networks Overview Start 9:51AM Monday
49		does freq mean no microwaves in ships ?

## Appendix H, GroupWare Comments

	57	Re: #49: NO. Depending on the frequency band, you may be dealing with microwaves. Generally frequencies above 3 GHz are considered microwaves. In fact, your standard microwave ovens operate in the 2.4 GHz range.
	61	Re: 49, Microwave ovens are only a problem if they are old and have leaks. Generally new ovens are not much of an issue.
	90	For #49, if you are referring to microwave ovens. Wireless LAN devices can be interfered with by microwave ovens, is susceptible to radiated emissions from microwave ovens but also conducted susceptibility thru power lines if not properly filtered.
51		What is the timeline of the standards development and how does it track with implementation requirements.
52		which is better Palm or CE?
	54	re:52 CE hands down.
	56	re 52: Depends on what you want. Palm is really only good for Outlook type activities. Pocket PC (CE) is much more powerful.
53		One of the greatest challenges in reducing manning onbd ships using wireless technology will be breaking through the status quo. We live and die by instructions and inspections. You cannot bring the ships an manpower saving application without modifying the policies of those groups such as ATG, PEB, INSURV, etc..
	64	re 53: great comment, there are too many accreditation pubs DoD, Navy etc, and many have different or conflicting requirements
58		Do you know that the freq range for 802.11 for Japan is? The 22 MHz channels for 802.11 is impossible to get in Japan and Korea, not an issue inside the skin of a ship at sea, but impacts land and pierside. State Dept will NOT even ask for approval.
59		Emission detection -> easy target?
	63	re 59: Depends on how far out the signal goes. Inside the skin the drop-off is only a few feet outside the ship. To detect 802.11 you would have to be very close.
	65	re #59; depends on the transmitter pwr. not really an issue unless in port.
60		where are other frequency comms in the scope of this ? I.e.; Irda and UWb.
	66	RE #60: The FCC rulemaking for UWB places commercial UWB development in the 3-10 GHz band. Again, unlicensed and under the FCC Part 15 rules. Not sure on the Irda.
	80	re 60 the roadmap is to help address future/near technologies such as you mentioned... the effort to date has been to map out the Tech Authorities/identifying policies and requirements such that new technologies will be able to navigate the T&E accreditation process and that we can plan better for their potential implementation.

## Appendix H, GroupWare Comments

67		FCC requirements limits 802.11 series to 100 milliwatts! Microwaves are 1000WATTS- even with minimal leakage - they exceed output of WLANs... Also the emissions of the CRTS are in the 100-300Watt areas - if we really consider EMCOM - all CRT/monitors must be turned off!...
	336	re#67: Another thing to think about is interaction with other systems.... some ships have an internal, low-power communications system. Basically it's a digital walkie-talkie system with an antenna running throughout the ship. Since they operate in more or less the same frequency band, it might be safe to worry about the communications system picking up the 802.11b signal and redistributing the packets
68		Need to run an experiment with wireless technology on ship and get P3's to detect.
70		IF we are worried about emissions off ship then why is Bluetooth not in here? If someone can sniff this, then is there a greater security problem ?
	77	re #70; I don't think it is a measure of being sniffed, but detection of a signal.
71		Please submit any fielded shipboard WLANs not listed on the slide.
72		Has IA approved this on ships???
	74	RE#72: Should be part of the networks C&A
73		Do any of the LANs use the SecNet 11 Harris product that is NSA Type 1 certified and also comes with freq conversion kits to move into approved military freq bands.
	75	re 73: CORONADO does
76		A Wireless network is installed on USS Elrod as part of the Wireless Expansion of ICAS (WEI)
78		is SECNET-11 the only WLAN type 1 device?
	86	#78- NO - Northrop Grumman has a "mounted" Secure 802.11b system - / Harris is the "dis-mounted" piece (Local area)
	333	Ref 86, If you are referring to the Northrop Grumman solution for a SWLAN certified to the TS, it is NOT NSA-certified for secure operations.
	335	re #333: then how is it being implemented
	343	Ref 335. I am not sure what you mean by how it is being implemented. Army has been told, along with Northrop Grumman and General Dynamics, that they are not to use the product to processed classified nor advertise it as such until it is NSA-certified. Regardless as to who it is to blame, NSA was not involved in the product and you simply can not take a product previously -certified in one environment and assume it is certified in another environment.
	345	re 343: Yes, agreed. I was under the impression that it (TS) was in use at this time without approval.
	346	re 343: any idea when it will be approved by NSA.
	349	Re 345, 346: Nope, they were told to not use the device for other than unclassified, sbu. I'll know more next Monday on the path ahead to get this product certified.

## Appendix H, GroupWare Comments

351	re 349: How do you tell the difference between SBU traffic and regular unclassified traffic on an unclass net (to my knowledge I don't think there is a way unless you are the initiator)....It seems to me that all unclass networks will eventually be FIPS 140 encrypted....
352	re#351: at the traffic level, none. SBU relies on document marking and the honor system on UNCLASS networks.
353	re#351: IPsec probably. It'd probably be an excessive load at the firewall though, having to encrypt/decrypt on top of content-filtering, proxying, and other.
359	re 351: an issue we are having with printers that print different classifications TS, SECRET, CONF. How do you tell?
360	re#359: the network it's joined to? You can control which network they're joined to. VPN's help.
361	re #360: Again, good for ships with space, how about subs. we don't have enough room to put another printer onboard.
362	re #351: Agree that IPSEC is current choice but AES will probably win out through time. Now we have just stated that all data across an unclass network/ WAN has to be FIPS 140.....This is a lot larger of an issue if we can control SBU info
363	re#362: IPsec is a network protocol which will probably end up using AES, which is an encryption algorithm
364	re#363: in fact, I believe it is available on some VPN's already
372	RE # 335. NSA has approved a GSM (Spectrum) handheld device with an integrated type 1 encryption. Build by General Dynamics (Motorola).
387	Re: 372 Yes, both General Dynamics and Qualcomm have NSA-certified type 1 mobile phones - one GSM and one CDMA. Unfortunately, they operate over circuit-switch data and providers are moving to IP. We are an effort to migrate these products to next generation cellular. Information on either of these devices can be found on <a href="http://wireless.securephone.net">http://wireless.securephone.net</a> .
408	re #387: Our Lab has performed assessment with soft switches as well, via Ipv4 exchanging protocols using Media gateways (TDM to PACKETS).
429	re# 387 : Currently all you need is a laptop and a small transmitter (about 6"x 8") to provide secure wireless voice communication, using FNBDT (NSA type 1) This is also a soft switch solution, no circuit switch required.
430	re #429: used in what application i.e.... in the field or onboard ships
431	re: 429: FNBDT?
450	re # 430 One vender (TELOS) uses an UNIX application, the other (vendor (IP ACCESS (NANO BTS)) uses a simple Microsoft OP, currently used by some DoD agencies. CECOM R&D has been assessing for GIG BE implementation. It is used in a Community of Interest (COI) architecture today.
463	Re 431: FNBDT - Future Narrowband Digital terminal is a set of specifications developed by NSA to enable circuit-switch telecommunication devices to interoperate in the secure Type -1 mode. HAIPE - High Assurance IP encryption is a set of specifications developed by NSA to enable INE (in-line network encryption) devices to interoperate.



## Appendix H, GroupWare Comments

	478	re # 431 FNBDT -Future Narrowband Digital Terminal, is a NSA encryption algorithm that replaced the STU-III secure algorithm, now we have the new secure Terminal Equipment (STE) that supports STU-III, FNBDT and STE.
	481	re 478: Encryption is one element. There is a MER - minimum essential requirements - a vendor must implement in order to be FNBDT complaint. The MERs are Baton encryption algorithm, MELP vocoder, key specification, and a modified 707.4 signaling piece. You can view FNBDT as an application. FNBDT products DO NOT interoperate with STU-3. STE interoperates with STU-3 in the STU-3 mode.
	489	re #481 exactly, however if need to reach a specific STU-III device, then a STE-R allows you to interoperate.
	492	re 489, Not sure if your saying STE could relay FNBDT. STE only works in one mode - STU3, FNBDT, or STE. The complaints we get into our office is our secure Type-1 cell phones do not interoperate with a STU-3. The Iridium is the only mobile voice product that interoperates with a STU-3
	519	re # 492, Not exactly, the STE versions 2.X (recommend version 2.2) do train for an end STE device configuration, as long as its in an "ENABLED" mode (FNBDT,STU-III and STE)....However a STE-R (where 'R') means remote does signaling exchange from STU-iii to FNBDT/STE. The STE is not a STE-R.
81		Will these initiatives fit into the JTRS Program ?
	82	re #81; JTRS????
	83	re 81: when is JTRS going to actually deploy?
	88	re 82, Joint Tactical Radio System
	92	re: 81 JTRS program is currently introducing a IP(v)6 waveform...
84		WJK - USS ELROD also has full a WLAN infrastructure installed. This WLAN is currently disabled due to the WLAN moratorium. Efforts to identify testing, etc that will enable wireless operation are ongoing.
87		JTRS does not deal with LANs on the Red Side router. They will only deal with offship comms, I could be wrong but just spent a day reviewing the AMF Cluster RFP.
89		wrong hull # for elrod
91		KSA FNC at ONR has Wireless WAN work on going...Intra Battlegroup Wireless Networking (on ESSEX ESG), Composite Networking, Traffic Flow Engineering, Dynamic Link 16.
	95	re 91: IBGWN on ESSEX is with VRC-99 radios at 100Kbps. It is not 802.11 compliant
	104	re 95 the VRC-99s were not suppose to be 802.11 compliant in the JTF WARNET or IBGWN applications. If you desire an extend conversation IBGWN please see Capt Kendrick during a break.
93		Army has been pumping bucks into JTRS this as well as their own wireless network.
	334	Ref #93, all the Services have been pumping money into JTRS. Army's connection into JTRS is WIN-T. Warfighter Information Network - Tactical.

## Appendix H, GroupWare Comments

94		JTRS Cluster 1 EDM waveforms will be available in the JTeLs in FY 06 for Cluster 1 to include the WNW and its 4 SiS.
96		how can we better coordinate sbir efforts among the military services ? ONR assist ?
97		Are these WLAN installs POR, who is sponsoring these installs?
98		Vince Piarulli Policy Start 10:10AM Monday
99		There is a "Wireless PLC" SBIR Phase II that has been awarded and not to be confused to Wireless PLC Interface SBIR Phase II
100		Help, I am lost in the acronym world, will there be some dictionary for some of these ?
101		Spell out acronyms on first use.
102		ONR KSA FNC is briefing OPNAV on the Enabling Capabilities for FY 05 and beyond based on the Gaps as determined during recent ops. It seems like this process needs to get this group better involved in determining those ECs.
103		KSA FNC Networking Projects' transition sponsors are PMW-179 PEO(C4I).
105		KSA? FNC?
106		KSA FNC - ONR Knowledge Superiority and Assurance Future Naval Capability
107		Who is responsible for establishing policy, acquisition, and ILS for the portable devices (wired or wireless) - if NMCI who pays?
	113	re 107: NMCI jacks the price up quite a bit on devices. For example non-NMCI Blackberry \$45/mo, NMCI Blackberry \$143/mo.
	116	re 107: Is MILSTD the reason?
108		Who is the originator of the WLAN Moratorium 192206Z AUG 03?
	112	Re 108 Commander Fleet Forces Command N6
109		Vince, The DISA wireless STIG is under a rewrite. The original STIG needed some work. If you email me, Anna Entrichel, I can send you the latest draft and the projected time of final release. You are certainly welcome to send comments to the STIG after reviewing the current draft.
110		what then is the process for getting a wireless lan on ship since there is a moratorium and no direct policy
111		I think there is also a DOD directive for Wireless Networks, I attended some of their meetings a few years back, Carl Cusamano at AT&L lead that effort. Probably need to see what they came up with as a DOD roadmap for wireless devices.
	126	re #111-More on Navy Policy is coming up on the agenda from CDR Larry Pemberton and I saw there was supposed to be a rep for the DoD policy. Don't know if they are present.
114		anyone know where I find "tempest" requirements today ?
	133	Ref #114, general TEMPEST rqmts can be found in TEMPEST 2/95
115		DOD RFID Memorandum, Oct 03 to satisfy CENTCOM tag all containers going into theatre.
117		Interesting... DoD policy forbids PDA device on DoD networks

## Appendix H, GroupWare Comments

	119	re 117: NMCI allows PDA Hotsink software...interesting
118		Vince, the final basic robustness WLAN protection profiles have been submitted to the NIAP for acceptance. I can send you copies if you wish. Once the PPs are accepted, 8500 dictates DoD must purchase products that comply with the PPs.
120		Vince there is an update to the NSA Apr Message. I believe the message was released in June 03
121		<a href="https://infosec.navy.mil">https://infosec.navy.mil</a> has many of these refs
123		Local DAA's approved PDA policy
124		ePMA uses Windows CE devices (Pocket PC). How is this since they are not approved to hook to the shipboard ISNS?
125		Vince, the PKI policy will allow for the use of commercial PDAs/Blackberry that implement a soft token PKI. If a hard token is required, then most blackberries, with the exception of the CDMA BB 6710, either have or will have a CAC reader designed by our office. More info, call our office Anna Entrichel.
127		Vince, the 8100.bb was supposed to be signed by Nov 30th, 2003. I can get you more info as to if it was indeed signed. Anna E
128		Wanda, I have a Virtual Program Office site for the NIIN, I could host the information on that site. See me at the break and we can discuss. Mike Stewart
	151	Re #128 - Mike, interested to hear what you have to offer. We are currently proposing to use NKO. Expected to be in production NLT 19 Dec. Will have a WLAN IPT or COI community under the Sea Power 21/FORCENet community. NKO provides vehicle for document storage and can be used as a communication tool for the group (chat, message threads, calendar, updates, etc.). Best part - it's at no cost to us. Thanks, Wanda
129		does the NIIN ipt still exist ?
	130	Re: 129 - yes
131		Note: Guidance doc applies to network infrastructure, not client devices. New doc for client devices to be developed. - LAF
132		when will this be approved?
134		Does WLAN include VoIP, data and video?
	137	re:134 WLAN on MASON is capable of VoIP and Video, but is currently only being used for ISNS unclass expansion.
	139	Ref 134, WLAN includes VOIP, data, and video. Harris for SecNet-11 can demonstrate it using a PALM and sleeve, as well as other WLAN vendors using a PCMCIA sleeve.
	140	Re #134: Yes although there are some different requirements specified regarding voice apps versus data apps. - LAF
135		There was an old web site for the NIIN that was de activated when we established the NIIN VPO site.
136		is that cart before horse?? need devices whether wired or not to improve processes
	144	Re #136: If that comment refers to cmt 136, we had to start somewhere and

## Appendix H, GroupWare Comments

		infrastructure was on the table at the time.
138		Is the NIIN VPO site on the SPAWAR VPO site? If you are members of other VPO sites at SPAWAR is this just another site for info?
142		The security software approved by NSA on the Blackberry was also used on PDA's. Where does this software stand now ?
	155	Ref #142: The only thing NSA did was to review and sign the software upon the Blackberry, as well as turn off items such as RF, microphone, etc. The PKI policy allows for the use of commercial Blackberry for now RIM "signs" their software. Realize this signature is by RIM and not by NSA. We are in discussions with HP and others to allow us to review and sign their sw. This signatures prevent other software from being loaded onto the device and the review gives us assurance that there is not any hidden software..
143		Emission detection (Cell tower) --->>> easy target!!!
145		So in summary, the WLAN implementations to date are only for intranetworking inside the ship on the ISNS, not to into ADNS for connectivity to other users outside the ship?
	149	Re 145: NETWARCOM is looking at 802.11g through ADNS ship-to-ship.
	154	Re #145: I know of some apps that work towards connectivity outside of the ship. Most seem to focus intraship, though. - LAF

## DoD Policy

MainC mt#	Ref: Cmt #	Comment
146		CDR Pemberton on 8100.bb Start 10:25AM Monday
	161	Re 146: WLANs seem to work surprising well on metal ships based on experience. Exactly why may not be completely understood but there are a lot of good guesses, mainly focused on the fact that spaces are not hermetic and signals leak through cables accesses, etc. Smartship has gotten full ship coverage on a DDG -51 class with 47 APs. - LAF
	162	re 161: Lance is correct. It is a misconception that WLANs won't work well on Navy ships.
	166	re:162 I am a happy customer and get full coverage onbd MASON. /RGB
	169	re:166 Did you buy your own PEDs?
147		How do we traverse the issue of wireless through several decks and bulkheads for Damage Control or Troubleshooting?
	150	re:147 Access points are placed strategically throughout the ship and powered via the Cat 5. Allows near total coverage inside the ship.
	152	re 147-navsea phila and usna testing complete showing rf barriers with steel and aluminum in different ship types
	153	re 147: Research has been done on ship WLANs. Several studies show that they work well in the shipboard environment and do go deck-to-deck.

## Appendix H, GroupWare Comments

	156	re 153: How many decks...i.e. can I communicate via wlan from a router at one end of the ship 1000 ft thru many decks and bulkheads.. where are the results for the test?
	158	re 156: During Industry Day tomorrow, stop by the Mobilisa setup and talk to Nelson Ludlow. He has a lot of data on this.
	159	re #150: and if one of those goes down, where is the backup?
	163	Re 156: 3eTI has done studies as well. There have been studies by NPS as well.
148		The NIIN VPO is on the SPAWAR VPO site, you need to notify the site administrator that you need access to a particular site to enter it.
157		DoD policy for wireless is for Secret and below only.
160		who has the DAA matrix ?
164		there are rf barriers if no cableway/open hatch in steel ships
	172	Re 164, 165: Obviously, thick metal will block RF. There is no magic solution to coverage. This is why we do site surveys when designing the network. It is why USS Howard had 40 APs but we went with 47 for USS Mason. We are also funding SBIRs geared toward developing design and survey tools to make WLAN design easier. RF in metal boxes is an issue. But, experience says it works fairly well. You still have to design carefully for each platform to assure good service. - LAF
165		Experience shows, onboard submarines, the use of handheld radios do NOT penetrate thru the Missile compartment bulkhead or the Engine room well at all.
	167	re 165: I guess that means they would need more access points on a sub.
	168	re 165: could be, need to know if a test is being planned for submarines
170		important brief - really need to get a copy of this before we leave so that we can debrief and distribute to our host commands asap
171		In fact HME experiences with wireless networks work very well, but at lower power levels due to reflected energy in the ship spaces.
	183	re 171 and 172 One aspect on ships is that the longitudinal framing acts as a wave guide, but tends to inhibit transverse propagation. Transverse bulkheads are sometimes barriers, but with the number of wiring penetrations sometime not. Access point placement is still not an exact science.
173		Yes, but what is "Knowledge?"
174		If you decide to radiate outside the ship for ship to ship extensions or flight deck, well deck for users that are exiting the ship; has any EMI study been done to see what interference happens for 802.11 with many systems in and around these devices (specifically radars, and at 300mWs you will not compete against bleed over from radar systems) and several aircraft systems will not want you radiating on flight decks anywhere around their spectrum.
	176	re 174: very good question, RADAR eats everything
	179	re:174 3ETi through the smartship office.

## Appendix H, GroupWare Comments

	186	Re 174: No formal studies, however, Smartship has discussed EMC with NAVSEA 53H, the EMI gurus and they have done an assessment that states 802.11b type systems have low prob of EMI issues. - LAF
175		Who installed the wlan on the Mason
177		Re the manning reduction issue: developing and implementing the wlan and applications are only two facets of the sys engrng approach to reducing or rather optimizing manning. The issue requires the ship design community as well as other disciplines to realize potential. The purpose served here is to build and provide a networks roadmap for awareness and the involvement of those that need to be at the table to realize that potential. The strategic approach that DoD promotes need to be broadened to include reevaluation via roadmaps or another strategic option.
	185	re:177- Navy AIT PO funded Wireless surveys (paper reports) across MSC, and most classes of ships today. Reports should be available by early Jan 04 as surveys are still underway thru Dec 03. Will be glad to share results.
178		So when you get into port do you turn of the WLAN networks?
	181	re 178: Encryption is the key here.
	188	Re 178: Unfortunately, encryption is only once piece of the puzzle. FIPS 140.1/140.2 only provides assurance with the encryption, you have other security areas that you need to be concerns with such as TEMPEST, goodness of the software, tamper rqmts, etc.
180		When 8100.bb finally gets signed I would expect a cascade of related policies to go into effect.
	182	Ref 180, they are currently working on the fact sheet and follow-on to 8100.bb to , hopefully, release soon after 8100.bb is signed
184		At 300mWs you probably could get by with using in port, but we have in the past reviewed waivers to use up to 100W amps to get WLAN coverage for larger surfaces ashore, and you can get those for the IEEE. It is an unlicensed area and you find MANY users playing in this area to include Mom and Pop cell phone providers that Jam you all over the place, this will be hard to use in the ISM bands outside of the ship.
187		Wouldn't a local DAA rather have it be accredited at the DoD level than go at risk and approve at the local DAA level unless it's for testing/development purposes only?
	191	Ref #187, 8500 mandates any connectivity to the DISN (i.e. NIPRNet/SIPRNet) DoD networks be approved by the DISN DAAs. A local DAA does not have the authority to connect , test, any connections to the DoD network
	193	Re: 187; Does getting software and hardware thru DITSCAP address and do these have to then have to become PPL from SPAWAR
	199	Re:187 The DITSCAP process will address connectivity issues but addition wickets will be required in order to get onto the PPL

## Appendix H, GroupWare Comments

189		The management of the spectrum needs to evolve as these devices proliferate. The current infrastructure; comms, radars, IFF, navigation, etc. have freq plans but does not accommodate these new devices. Also, the below decks use of frequencies will need to be coordinated if you have multiple voice and data devices for various purposes such as admin, HM&E, training, etc.
190		re manning reduction, wireless technology is enabler for workload reduction which leads to manning reduction via manpower analysis. e.g. how many yeomen do we need in an aircraft carrier if officers and senior enlisted are doing all admin themselves wirelessly ? how many secretaries do we have in our offices now that we are web-enabled ?
192		There is no longer the provision for Operational DAA to approve connections vice a developmental DAA. So the CIO for PACOM is not going to be able to approve use of systems without DISA approval first?
194		In reference to the discussion of PDA/PED, NSA lead a study for the Pentagon on issues surrounding PDA/PEDS. It is available at the TS/SI level
195		Reducing workload improves your "standard of living" aboard ship. Giving me more work to do because we reduced manpower does not
197		I think interference will become more of an issue as more devices and applications for those devices are identified.
198		Sounds like we need a discussion on the DAA process
	200	Ref #198, DISA has a CD regarding DAA and their process and I have a copy of it back in my office, Anna E.
	201	Re 198- Would think that the DAAs, both OPS and developmental need to be involved and aware. The strategic motivation for both to be involved is important.
202		Vince, maybe I missed it, but, I was not sure if you wanted to include NSA's IA advisory on wireless networks and commercial laptops into your brief. Anna E

## Issues Discussion

MainC mt#	Ref: Cmt #	Comment
203		Glen Hoffman Wireless Network Issues Overview 10:55AM Monday
204		If we go wireless, do we go completely wireless or keep the old "wired" infrastructure around for a backup? How does this impact manpower reduction if we have both?
205		Move wired drop on a ship = \$5K; Move 64 wireless drops on ship = \$5K; you pick
206		are they mutually exclusive? there are benefits to both

## Appendix H, GroupWare Comments

	210	re 206: True
207		For CDR Pemberton or Lance - where can I get more info on how knowledge mgt will be used to evaluate "acceptable uses of wireless devices?" We have a number of wireless apps under development, and several different wireless devices are being considered for deployment of these apps. Knowing what the KM evaluative criteria are would be helpful. WJK
208		In mid-spring 2001 - COMTHIRDFLT sent a message to SPAWAR - Stating that WIRELESS was a critical fleet Requirement. What else did you need from the fleet?
209		T-AKE ORD requires an advanced cargo inventory and control system. This was written into the ord specifically to require a commercial Warehouse Management System. There are hundreds of these systems and they have been wireless lans for over ten years. This is not new technology. But to be implemented in the Navy policy needs to be aligned.
211		Sometimes the requirement get into the Objective vice Threshold requirement and gets lost in a cost/schedule discussion so wires stay. Many aircraft systems seem to be going to an all optical network aboard, I know that AFRL has some of these platforms, is that another roadmap for the future for LANs? Or are we only looking at wireless?
	218	re 211: optical is wireless...however, are we looking at optical and RF or RF only
	220	re 211: how well does optical work through bulkheads,...hmmmm
	223	re 220: Optical networks would be excellent for intra-battlegroup connectivity and ship-to-air connectivity. This pushes the throughput up to the Gbps range.
	226	re 223: agreed, but what is the cost compared to RF
	229	re:220 and 222; thought that this was looked into by the BG AME? Does anyone have the results on using opticals between ship ?
	230	re 226: Researching the cost. However, with the need for increased bandwidth, Gbps is much better than Mbps (802.11) and the Kbps (VRC-99).
	233	re 230: Bandwidth is def. an issue that needs to be considered. We need to meet the needs of bandwidth for the year 2020, not today.
	238	re 220 & 223 - BG-AME did not consider optical technologies for inter-ship connectivity. Rather, UWB radio was the technology originally considered. For BG-AME, the question is OBE because BG-AME shifted to intra-ship focuses. WJK
	239	re 230: in T-AKE we have a separate LAN for the WMS...in addition to an ISNS. Major concern was bandwidth
	240	re233: Bandwidth is an issue, but every single BG commander coming back from OIF, when asked by higher, said they had enough bandwidth to do the job.
	244	re 240: that's all good for today, but when you start video conferences and future applications, then what?



## Appendix H, GroupWare Comments

	245	re 244: I agree. The BG commanders need to state the true state-of-affairs WRT bandwidth and not sugar coat it for higher.
	247	re #245: yes, guaranteed there is a LAN Administrator pulling his hair out trying to figure out how to give his CO more bandwidth.
	252	re 247: There are NOCs that are pulling their hair out trying to give the BG bandwidth as well. NCTAMS EURCENT said that during OIF there were a few near-misses on total loss of bandwidth due to overloading.
212		anyone know the new terms for mns and ord ?
	213	re 212: what were the old terms?
	214	Re #212 - ICD - Initial Capability Document (WH)
	215	Ref 212, MNS - Mission Needs Statement, ORD Operational Requirements Document - both replaced with ICD see #214
	216	RE #212; ICD is the new MNS, and CDD (Capability Development Document (CDD) is next step typically down with the ORD.
217		urgent requirements msg from Fleet to opnav would do it
219		woops, Fleet urgent requirements to Fleet ??
221		Need the fleet requirement generated via the COMTRDFLT message into an ICD or inserted into current ICDs to support the acquisition community's procurement of wireless.
	224	re 221: Wireless doesn't mean intership only.
222		We need to pay attention to our customer like the USMC and their wireless needs.
225		Re optical and RF: Yes, many different mediums are being considered. In Smartship with are working on Diffuse IR and Ultra-wideband, as well as looking at 802.11. We are also looking at 802.15, .16 and 1451.5. There are many potential beneficial technologies. - LAF
227		the real innovation is in the application
	234	Re 227: This is true and key. Of course, if you build it they will come. Problem is a chicken and egg situation somewhat. Can't completely spec the apps without knowing something about the capabilities of the infrastructure. But, can't design infrastructure correctly without some idea of what apps will run on it.
228		Optical forum at NRL tomorrow for free space optical networks to include sub-surface. See John Kuchinski if you want info on that workshop. Optical inside the ship in my mind is wired in most instantiations since we need fiber. Optical or RF over fiber is still static. A hybrid arch with some fiber as infrastructure with wireless drops seems to be the direction folks are moving.
231		Will there be an NCR for wireless ?
232		Warehouse Management Systems (WMS) have to be wireless. They direct forktruck movement throughout the warehouse (or the shipboard cargo handling areas). The data is collected using bar code readers.
	235	Re: 232 you may want to see what NAVSEA Phila is doing with the Smart Stores project.

## Appendix H, GroupWare Comments

	236	re 232: How is it done today if not using wireless.
	241	re 232: how does the forklift get to the part if the network is down (i.e. from a virus/worm)?
	242	re 241: We go back to paper based direction, as we do business today
	243	Re 241, that is an inherent issue with wireless - DOS attacks and jamming. So, how do you deal with it is a question to be answered.
	246	Re: 241- Most systems also have barcode - local process and remote download or cradle synch - you do not have to be ONLINE all the time... This is how we all work when the network is down - we still to local machine processing.
	251	re 232 and 236; manually and on Carriers with lots of manpower for load out. Recent study on strike up/down showed significant accuracy of throughput by using automatic identification technologies/automatic data capture in the "as is" business process. Study shows potential for approx 60%or greater reduction in man power in going to the "to be" business process and take full advantage of AIT/ADC tools. However in order to get to these reductions this requires the WLAN be built into the ships infrastructure.
	256	RE 241:246 see 251
237		Not one method is correct. A prime capability of FORCENet is Dynamic Multipath Survivable Networks. Therefore, there is room for multiple data paths to include RF and Optical offship.
248		<p>Comments to Vince Piarulli brief:</p> <p>Virginia Class will only have NIPRNET wireless LAN onboard at delivery. It will be modified to bring it in line with PMW165's SubLAN wireless network being installed on 688/688I platforms at PSA for hulls 774-777. SSN778 will be SubLAN compliant out of the box during new construction. Currently SIPRNET is on hold until the prohibitions are lifted and further testing is completed. Wireless testing is just beginning with NAVSEA 08 to assess wireless implementation for the engine room, SEA08 is interested in SIPRNET wireless but requires testing to insure reactor plant instrumentation is not adversely affect.</p> <p>USS Norfolk wireless LAN was installed by Trident Systems under an SBIR sponsored by PMS450. It operated onboard for over a year, it was well received by the ship but was removed at the direction of SUBLANT (Tom Nutter) once they found out it was operating on the ship.</p> <p>Trident comment:</p> <p>USS Alaska and Alabama had prototype wireless LANs installed in the missile compartment, but they were removed or shut down upon completion of the test period.</p>
249		who are "the tempest people " in navy ?

## Appendix H, GroupWare Comments

	257	RE #249: COMSPAWARSSYSCOM SD is the CTA for TEMPEST in the Navy. TEMPEST folks at PAX deal with them regularly. I can get you POCs, but do not have off hand right now. See me during conference or email later. Scott Hoschar , NAVAIR.
250		I imagine that the PACOM directive did not include Coalition, when they are basically coalition for everything that they do, they will not be Type 1 with every wireless device in a JTF.
253		What is IPV6 in a nutshell?
	255	re 253: Internet Protocol Version 6 is the next generation of IPv4. It is not backwards compatible to IPv4 and has a much longer header for routing.
	347	re#253 & #262: IPv6 is the "next generation" IP addressing scheme. It is supposed to relieve the shortage of available IP addresses in IPv4 (which is what we use now) and is also supposed to be "more secure".
254		Can we print certain comments or get a copy of the days comments at the end of the day
258		Scott, the TEMPEST folks are in Charleston, I believe, we can check with Kathy. Mike
259		mason case study brief needs to address what's left to do wrt issuance of test report
	260	re:259 EMCON testing is addressed in the Case study... will talk to any specific issues not covered in slides themselves...
261		Need to coordinate and collect emissions during an exercise (using P3's etc...)
	272	re 261... are more than willing to do so from a Smartship perspective... Lessons Learned from initial foray into developing those tests is working around ship schedules, range availability, and technical equipment issues. We are open to conducting more thorough tests and leveraging our efforts to other ship classes as well... DLB
262		IPv6 can address to IPv4 devices, but you cannot do it the other way. JTRS Cluster 1 with WNW will NOT be IPv6 compliant. It will come in another Spiral of JTRS or maybe in the AMF Cluster for the Navy and Air Force. It would have cost millions to amend the current contracts for JTRS so they will not make the mark stipulated by ASD NII, at least as of today. You will end up with v4 and v6 running in parallel which a Cisco router with IOS 12x can do today.
262		IPv6 can address to IPv4 devices, but you cannot do it the other way. JTRS Cluster 1 with WNW will NOT be IPv6 compliant. It will come in another Spiral of JTRS or maybe in the AMF Cluster for the Navy and Air Force. It would have cost millions to amend the current contracts for JTRS so they will not make the mark stipulated by ASD NII, at least as of today. You will end up with v4 and v6 running in parallel which a Cisco router with IOS 12x can do today.
263		On T-AKE we are not building a pilot. We are building 12 ships with WMS.

Appendix H, GroupWare Comments

264		Frequency and health issues need to be addressed (HERP) when using many wireless devices in an enclosed space such as ships compartment.
265		Of note, when the administrator turns off the access points, the client devices go into full power search mode.
	267	re #265: yes, however, no data is being passed without handshake/authentication
	271	re 267: Speaker was talking about EMCON policy.
	274	Re: 265, This is the specific issue that I was referring to, we are attempting to figure out how to control the end user device emissions so that we can use wireless devices at all times afloat. Oster.
	276	re #274: Train the end user
	278	re 276: You're assuming that the wireless machine is manned when it is on.
	280	re #278: Good point, yes I was
	283	re 280: If we moved to a thin-client approach to computer systems, then you wouldn't need to have the computer powered up all of the time.
	286	re 283: why does thin client make a difference with whether device is powered?
	292	re 286: Sun Microsystems has a wireless thin-client system that keeps a users session current even when the client is powered down. Therefore, when you power up you are right back where you were working. The main reason Sailors leave their computer on is to keep their work up for easy access.
	298	Re: 292 If you are in an NMCI seat , you must leave your computers on (but logged off) on a 24/7 basis to receive the security and upgrade pushes....
	300	re 292: NMCI is not thin-client. It is very fat-client.
	301	re # 292 - Just how fat is it!
	302	Re 292. Obesity is an issue in this country. Why should our IT be different.
	303	re 292: 12 billion fat
	308	re 292 NMCI is doing a pilot to look at using ultra thin clients.
	310	re 308: Thin and Windows = oxymoron
266		No the P3 are collecting the data on the ships with the wireless
	268	Re: 266 can you send more info on this?
269		The NOSSA letter that grants HERO approval to 802.11b devices does not apply to magazines and weapons assembly areas. Any 802.11b devices used in such spaces requires NOSSA approval and may require additional HERO testing, even if the equipment has already been HERO tested. POCs are Chuck Wakefield at NOSSA and Chuck Denham at NSWC-Dahlgren. They are currently working on clarifying this issue as it is not self evident in the letter.
270		All wireless use in shipboard environment - once it is finally accepted as a Program - will have CONOPS and TTPs... Training and shipboard standards will address 90% of the EMCOM and Security concerns.

## Appendix H, GroupWare Comments

273		Power over Ethernet also brings up an electrical isolation issue for the engineering spaces. They have from 20-50volts going into them. They need to be able to be isolated during a lube/fuel oil leak which in effect negates the WLAN in those areas. This shuts the door on any damage control applications or monitors which would ride on the WLAN during that casualty. Alternative would be to come up with an acceptable solution to the engineering inspection community./MASON EMO
	277	Re 273 - one option is to power the access points conventionally, rather than POE. We had to do this for four access points onboard ELROD, albeit for a different reason (100 meter Cat5 length limitation was exceeded). Another option would be to provide individual isolation for each access point in machinery spaces, which would trip the given access point off the network without adversely affecting other access points. WJK
275		Re: 273- Not necessarily - can go with local power to machine spaces APs and in emergency (DC event)) have an open system and do ad-hoc vice infrastructure...
279		Who is going to change the training manuals and appropriate instructions in order to get the paradigm changed toward wireless tools?
	291	Re 279 - part of the responsibility of installing a WLAN is to provide ILS support which includes training on the tools as well as changes to the ILS documentation that leverages the powers of the WLAN and its apps. Examples are to trigger Planned Maintenance based on wireless HM&E data acquisition. Another is to embed wirelessly-acquired real-time HM&E online signal data into the troubleshooting section of a TM loaded on a handheld computer..
	299	re279-as the particular project technology is transitioned from Smartship to SPAWAR via a transition plan, the training, tech manuals, network admin, etc. will be addressed via associated document(s) for the community to chop before final approval.
281		From a submarine standpoint, we just need more time on the platforms/hulls to run wireless LANs, this will be a learn as we go process. NIPRNET is a low risk venture from an IA standpoint - we need to get through the current hurdles so we can see where the real problems reside.
282		Vince, there are issues with WPA, 802.11i. We are involved within the committees. I believe Rob Campbell is one POC. One must also realize that from an equities perspective, NSA is involved in understanding the technology, but not necessarily plugging up all the holes.
284		new NEC required when we migrate from fiber to wireless networks ?
285		Does your implementation interface with the INM? Do MIBs currently monitor Link Status metrics for WLANs? I seemed to remember that Univ of NH was the certification site for 802.11 compliance, because not all 802.11 system (APs and Clients) work perfectly together. A good test is to take a variety of clients and use them with a vendors AP that is not the same and see what happens. I know that when you use Harris's SWLAN you will be tied to that vendor only.

## Appendix H, GroupWare Comments

	288	re 285: Being tied to one vendor is unacceptable. With standards-based systems we should be able to choose vendors.
	290	Re 285: This is the old military - COTS dilemma. We want COTS for cost savings but... we then add on our own requirements that make COTS untenable. No easy solution. Interoperability will continue to be an issue. We just have to be as common as we can and live with the interoperability issues. - LAF
	293	Ref #285, Univ of NH has the gold device; however, one weakness is it does not test beyond 40-bit RC4/WEP. We've tested various APs and WLAN clients and ,yes, they do not interoperate very well and (hardly) none at all in the 128-bit WEP. Harris's SWLAN uses NSA type-1 encryption and we (NSA) are looking at in providing interoperability standards as it relates to IP and low-bandwidth applications (PED/PDA/future SWLANs, etc.)
	294	re 285 and 288, so far only one vendor has or appears to be developing an NSA type one approved 802.11 based wireless technology. So for the near term, that is the standard. Unless we want to buy the technology and put it in the public domain.
	295	re:285 & 288; this would support the open architecture issues, but where will we go to get all of the products that come with FIPS 140.2 certification, meets HERO etc. will there be a single/central point to get confirmation/approval to use ?
	297	Re 294: The point is, it is not really 802.11b. It is 802.11B-like.
	304	Re #294, the Army contracted with Northrop Grumman to build a SWLAN to the TS/SI level. I am in the process of having it NSA-certified and am not sure of how long it will take to have it certified. They basically took a KG-235 and embedded it into a chassis with some other components. I will say the solution is expensive (10K and up). ZAE
	305	Re 304: 10K per AP? Client?
	306	re #304: we still need an approved TS LAN. We as in NAVY
	312	Re 306, if cost in not an issue, then Navy should have a solution sometime this year. This device is a high-priority and I will do my best to get it certified. I will send out a message once the device is NSA-certified.
	315	re 297, NSA has indicated that 802.11 standards will never be type one certified. So all the type one 802.11 based solutions will only ever be sort of like the base standard.
	318	Re 315: Yes. It is the COTS vs. military Requirements issue.
	325	re 315: That's why we need and 802.11M (M-military) that is an military standard that multiple vendors can build towards.
	326	Re 325: Noooooooooo! :-)
	327	re #325: wow, what a concept
	329	re 325, I guess we need another milspec
	331	re 327: Sarcasm noted.
287		With regard to multiple wireless networks, this leads us to the much needed aggregation study to monitor/maintain the RF spectrum on the ship.

## Appendix H, GroupWare Comments

289		Regarding wireless policy issues, a big one will be the policy to use unlicensed wireless systems or equipment for; 1) critical Command and Control networks, 2) tactical or strategic missions, and or 3) protection of human life or protection of high value assets. Typically the systems and equipment we are talking about here this week are unlicensed equipment. Unlicensed equipment under both FCC (regulates commercial use of wireless systems in US) and NTIA (regulates Gov use of wireless systems in US) is an unprotected service. In other words, if any of these systems cause EMI or interference to authorized users of the spectrum, the unlicensed systems will need to cease operations. The same applies if the unlicensed system receives EMI or interference from an authorized user of the spectrum, i.e. the unlicensed LAN system must accept that interference. This makes a coherent systems engineering approach to the integration of a wireless LAN aboard a ship, that takes into account electromagnetic compatibility (addressed under technical issues), is critical.
296		we lost the bubble with the proliferation of wired LANs in our ships because no policy required the stovepipe programs to talk. we need policy to preclude another generation of dis-service to the ships.
	311	Re: 296. It starts with the local DAA and his IA staff (ISSM and ISSOs) to manage the configuration of their networks. Wireless has to be treated as part of the DAAs systems.
	313	re #311: Agree, however, they need guidelines and policy to cover their backsides.
	316	re 311: if the DAA wants it bad enough, he will do what it takes to get it...does the ISSM have the knowledge and expertise to provide good risk assessments
	319	re 316: and this is why systems are removed from ships/subs
	324	Re 313: That is where DoD, SECNAV, NETWARCOM and Marine Corps policies and the requirement for KM comes in to assist that staff. Forums such as this assists as well
307		Does the WLAN under C4I include the needs of the Medical communities bandwidth needs?
309		Agree we need a single program office for wireless LANs, just know interfaces with combat systems and H&ME.
314		WLAN coexistence is a major issue. We need an approach to deal with this, especially on a ship. - LAF
317		Has cost comparison been done regarding current shipboard LAN install/maintenance and support vice wireless for CAGs? - since we have never been able to fulfill Air Wing drop requirements on the CVs, I'd be interested in a cost analysis
320		We (Navy / Marine Corps) need to somehow get down to one wireless PDA which can access the shipboard and/or ashore WLAN. 2 and 3 devices are still too expensive, unwieldy and difficult to accommodate.

## Appendix H, GroupWare Comments

	328	Re #320. With technology changing so fast, you can have one PDA but realize it will be obsolete very quickly. Right now, carriers are migrating to 3G standards (WCDMA and CDMA2000). There are not too many devices supporting these standards.
	348	re#320: it needs to be sailor-proof
	354	re #320: define sailor-proof
	355	re 354: ITSN Jones needs to be able to do it with little training.
	357	re 355: ITSN = Information Technology Seaman
	358	re#354: Sailor-proof: no moving parts, no breakable parts, able to be tossed in a tool bag or dropped from the 03-level without sustaining serious damage. At \$300-500/device, they've got to hold up to some punishment.
321		roadmap needs to include governing body to take on policy and operational procedure issues wrt ALL wireless networks shipboard
	323	re #321: DISA???
	330	re 321: DISA - Defense Information Systems Agency
322		Submarine wireless LANs should all be coordinated by PMW165 and the planning yard. The planning yard needs to guard the submarine RF door to manage the aggregate RF on the ship to minimize LANs from stepping on each other. The key factor from a submarine standpoint is the SHIPALT or TEMPALT and how effect the planning yard is in maintaining control of the configuration envelop for each ship.
337		More EMCON/TEMPEST thoughts - How will other wireless devices play a part...i.e....printers, scanners, keyboards, mouse....etc.? Does a wireless printer authorized to process secret need a CAC or PKI to print? How do you secure a wireless keyboard? If I can "sniff" a computer output, why not a keyboards keystrokes or the input to a printer?
	338	re#337: For Secret content, I'd assume that you'd have to have a wireless printer capable of Type 1 encryption.
	339	re #338: Is there one out here? Who is investigating?
	340	re#339: I'm basing that on the requirements in 8500.bb
	341	re #337: Policy should include these devices.
	342	re#341: I agree
	344	Ref 338, 339, what comes to mind is Bluetooth (802.15) where a particular blue-tooth device (i.e. computer) have a list of profiles (printer profile, fax profile, etc.) they can communicate. NSA is not (yet) involved with developing solutions for 802.15.
350		I'm getting into this a bit late (moved out of the peanut gallery during lunch) but one possible solution to the limited number of wireless devices you can use is to drive the AP into "bridging" mode. There's talk that it allows a higher number of devices and also allows the device to wander between access points if they're in the same address space. Trade-off --> security.



## Appendix H, GroupWare Comments

	356	re #350: and what of different classifications of LANs using the same "bridge" device
365		When I hand out a document/memo/instruction, it must have classification annotated on the document itself....5510.36 series....where is the documentation for email/e-documents?

### Methodology

MainC mt#	Ref: Cmt #	Comment
366		John Nolen Presents Survey Results 12:50PM Monday
367		John Nolen presents Methodology 1300 Monday

### Case Studies

MainC mt#	Ref: Cmt #	Comment
368		usns or uss coronado ?
369		One of the things to define: the requirement for justifying the use of wireless. Example: Does the watchstander who measures tank levels need to report via a wireless network or can he get by with a PDA which he periodically drops in a cradle and uploads the data?
	371	re 369: Why is a watchstander measuring tank levels? Shouldn't they have an automatic measuring capability?
	374	re #369: Are we saying that paper logs are no longer needed?
	376	re#371: Don't know. Bad example?
	377	re 369: TLI's are now being monitored and reported out to watchstander stations....They can also level the tanks electronically as well.
	380	Re: 371, Because we have had spaces flood as a result of the automatic level detectors not working.
	382	RE #369: Excellent Point ... the key being, define the requirements ! And assess the requirements to really determine if a wireless solution is needed. Let's not install a wireless LAN for the sake of installing a wireless LAN. I assume that was your point. (ooops . . comment was also just made by speaker).
	384	re#380: on older ships, watchstanders are used to verify automatic readings

## Appendix H, GroupWare Comments

385	re 369: Currently on ICAS ships, engineering log sheet data is manually collected via a PDA, then uploaded to the ICAS network via a PDA cradle. If the PDA is enabled to wirelessly access the network, the sailor no longer needs to synch up via the cradle. Also, the approval of the log sheet can be accomplished wirelessly by those in the ship's chain of command. This is a huge timesaver, because the log sheet data is usually collected once/hr. Also, it frees up the ICAS workstation for others to use. WJK
386	re #380: spaced have flooded from human error also.
389	re #384: In aviation we rely on the automatic readings. I don't understand why ships don't do the same.
393	re: 369 Army is also doing this on prepo ships and updating logs back stateside. They did this for their tracked vehicles to start. Would be nice to see how far they have progressed.
396	re 389 The amount of engineering put into ships is much less than put into a/c.
399	re 371 - automation of tank levels is one of the costliest logsheet readings to automate. Presuming a radar TLI is to be used, the tank would require gas-freeing to determine if the sounding tube is useable as a radar waveguide. Most likely it isn't (due to perforation diameter and bend radius reqts), so a new one would need to be installed, incurring a large design expenditure.
402	re 396: If we continue to dismiss technology because we need human backup, then we might as well get rid of GPS and go back to drawing lines on paper charts to figure out where we are.
405	re#402: one of the tenets of contingency plans: have a backup
406	re 402: we still us paper charts to plot the gps position
407	re 402: lets not just throw systems on ships without extensive testing. What other Back-up is out there instead of human intervention?
409	re 402. I am not dismissing technology, just noting the level of funding required to get it right so sensor inputs can be relied upon. And lines on the chart are still being used. But the sextons are at least gathering dust.
410	re 407: I said technology gets DISMISSED because of the requirement for human backup. If you read the 400+ posts here, many time someone has said, "what happens when it fails?" That same mentality is why some ship CO's were resistant to use GPS. They didn't want to rely on it in case it failed.
411	re 409: sexton use...PMS and Pre-underways
413	re 410, are they wrong in a zero defect world?
417	re 413: Yes, CO's who refused to use GPS because they were afraid it would fail were wrong.
420	re#409: Sensors are devices that usually convert either a physical measurement to an electrical signal. They almost always involve moving parts, which eventually wear out.
422	re 413: nothing is 100% and we need to ensure we have a back up plan for the fleet. Might want to ask my friends of the Cole

## Appendix H, GroupWare Comments

	427	re #422: Agree, in the sub force, we have backups for anything that is safety of ship. whether it be manual readings or another electronic sensor to determine the correct reading. Which brings us back to manpower. Just because something is easier "wireless", we cannot just remove the bodies needed to do the manual jobs.
	452	re 422-would COLE have had a higher situational awareness and better reaction using wireless (both hw and sw)? Hard question to answer but I'd like to see the ships have an improved possibility/probability of survivability with technology. Looking for the higher payoff for them is the way to go.
	453	re 452: all good, as long as we have a backup
	455	re 452: I believe they would have. The DCA could have received video from webcams from the DC team there as well as status reports, personnel reports, etc.
	456	re#453: Yep. It's why we still teach sailors how to swim.
	457	re 453: Wouldn't the backup just be the old way of doing business. I.E. GPS falls to paper navigation falls to the sexton...etc.
	460	re #455: Don't get me wrong, I am not an opponent to progress and new technology. I just don't want a system or policy to be implemented onboard a submarine or ship that endangers personnel. I have seen too many systems put onboard that are not used due to the trust factor or make it harder to get the job done then was before.
	464	re 456: too bad we can't access the web from here
	465	re 464: Web access while chatting would be nice.
	467	Re 465: This is a classified facility. No internet access.
	469	re 467: I work in a "classified" facility and I have internet access.
	470	re 467: interesting, our classified spaces have NIPRnet access
	471	re 469: not on the same system I hope
	474	re 467: How do you do research without NIPRnet?
	477	re #464, 465, 466, 476 - Not really. If web access were available, then we'd really lose your attention! See what I mean. On the other hand, we could use it to verify what some of these speakers are saying! Maybe we should check Google on the "how to's". Google has everything you know.
370		in flux...TBD
373		If you do the infrastructure right then take advantage of the automatic measurements....
	379	re 373: Correct! You can have the system automatically update a replicatable DB that replicates to higher via the NOC...no more message traffic either.
	383	re 379: no more message traffic at sea or just in port. What pipe is being used for subs? the bandwidth is still an issue for that (sub) platform.
	391	re 379: if no msg traffic, how do you access the data?

## Appendix H, GroupWare Comments

	395	re 391: For example, the automatic readings can be reported to CAS (Collaboration at Sea) which replicates to the big deck and the NOC. You can access the data on your local CAS server.
	400	re #391: and for subs
	404	re 391: I understand the need of other commands to view maint. data but the ship's still need to be ones to control their own destiny
375		CNO has changed his mind... USS CORONADO will be 're-commissioned' in the near future. Will have O-6 CO....
378		Dave Bartlett Smartship Wireless Case Study 1305 Monday
381		Has anyone done the studies in how "bandwidth" will be needed for the ships? What's the worse case scenario?
	388	re #381: submarines are the worse case scenario for bandwidth
	390	re 388: Agreed
	392	RE #381: Are you talking bandwidth in total per ship/hull, or wireless LAN bandwidth requirements ?
	394	re #381: I think Mine Warfare is in the same boat
	397	re #381: both
	398	re: 381; total ship and WLAN is subset of this.
401		Wireless helps for those sensors that would be hard to locate and run cable, long cable runs, band bends to get into difficult locations. There used to be ONR programs that I remember that even had the wireless sensors in propulsion systems to give remote feedback of sensor data.
403		There are C4I BW studies.
403		There are C4I BW studies.
412		I'm still confused about wireless sensors.... Yes, you save a couple hundred feet of Ethernet cable but you still have to run an electrical cable out to the sensor.
	414	Re412: We're working on that. Energy efficiency, power scavenging, etc.
415		This case study is a great opportunity for DoD KM process
416		Co's rejected the Navy Tactical Data System (NTDS) in the 60's
418		IEEE 1341 sensors was being modified to provide for wireless transmission. Any idea what the status of this is ?
419		Can you provide more information on the dynamic key exchange? I'm running a wireless network with 250 users with laptops and have only been able to use static keys. Dynamic key exchange sounds manpower intensive. Is it?
	423	re#419: Dynamic key exchange sounds like session key negotiation. Is that what you're describing?
421		The 3ETSI solution, aside from FIPS-140-2 certification, is it NIAP-approved? 8500 (I believe) mandates products meet any protection profiles (PP) accepted by NIAP. WLAN PPs should be accepted sometime by the beginning of next year.

## Appendix H, GroupWare Comments

424		As we go down the path of technology development and assessment and the possible introduction of a new piece of wireless RF technology into a ship environment, we need to remember that any modification to these wireless systems away from how they were sold, i.e. addition of directional antennas or power amplifiers to increase range and/or connectivity, will open another whole bag of worms regarding the regulatory world and "authorized" use of these systems by the Navy.
	426	re#424: Some manufacturers are more amenable (sp?). See Buffalo's wireless products (separate specialized antennas)
425		It would help in making the transition to " wireless" a part of the education process at our Naval Academy and other Education facilities. Train our leadership..
	428	re 425: You hit it on the head. Leadership buy in is needed.
	433	re:428, is there a leader today that does not use either a cell phone, a Blackberry and or other wireless device ? Seems like we need to encourage them to look a little further.
	434	re 425: Both Naval Postgraduate school and the Naval War College use wireless technology to provide network/Internet access for its students. Also, WestPoint went "wireless" almost a year ago.
	436	re 434: Academia using something doesn't mean it is endorsed by higher Navy.
	437	re #433: it is not just the leadership...it is policy. Policy dictates what we use/do in our workspace.
	438	re 437: Leadership sets policy.
	440	Re: 434 so now when these Officers go to the Fleet they will have to be frustrated by not having this capability afloat? Is this a morale/retention issue for new officers?
	442	re#433: but they also need to know how it works and what shortcomings are inherent in the technology
	445	re #438: funding dictates policy
	447	re 445: Who dictates funding?
432		usna will be invited to summit II @ npgs in may/june
435		Concerning the use of SECNET-11 on a permanently installed classified network. One of the shortcomings we immediately noticed was that the "part" the holds the encryption key is removable from the mounted base.
443		So we have to certify all products for FIPS 140 and Common Criteria for all products.....Then we have to go around and certify for each ship class for EMC/EMI.....So much for speed of technology to the fleet. We have to find a more robust process....
	444	re#443: don't forget HERO!
446		Who do we go to when a vendor comes in and says I have the "certs" ?
	449	re#446: PMW-161 is NETWARCOM's certification agent.
448		what is the "NIAP" process?
	451	Re: 448 Please define NIAP and EAL. Thanks

## Appendix H, GroupWare Comments

454		common criteria info can be found on <a href="http://www.commoncriteria.org">www.commoncriteria.org</a>
	459	re: 454 Thanks.
	485	Re 454: Also try doing a search on NSTISSP No.11 or NIAP Evaluation. There is a NIAP web site that describes the NSTISSP No. 11 program. NSTISSP No. 11 is a Federal requirement. DoD Instruction 8500.2, in Enclosure 2, details how DoD will implement the NSTISSP No. 11. The DoD policy is very flexible, with the ultimate intent being evaluating IA and IA enabled products
458		NAVSEA 05L has the DCAMS - DC Auto Management SYs - wireless & WebcaM - WIRELESS package with wearable computers built into the Firefighting gear. See BIW and NAVSEA for specs... System has been tested in the field.
	461	re:458 so is SEA 05L going to build out the wireless LAN so their wearable PC's can be used throughout the fleet?
462		NIAP info can be found at <a href="http://niap.nist.gov">http://niap.nist.gov</a>
473		461 -BIW&NAVSEA 05L have been waiting for 2 years now for the final decision on shipboard use of WLAN... It has an acquisition path - just not wireless PERMISSION>
479		Any idea what antenna/test set was used in the tests?
	480	re 479-Lance can answer what the RF test engineer used and we have lessons learned. Believe Dave is speaking about this now.
	482	Re 479: Can answer later. See me. - Lance
490		For 802.11b HERO/HERP/HERF accreditation, it was noted that it doesn't apply for weapons assy and magazine spaces. Is there a distance-from-source limitation given in this accreditation, i.e. 6 ft from the magazine space? WJK
	494	re#490: On carriers, the mess decks periodically are also weapons staging areas
	497	re #490: Submarine...all I need to say. always close to weapons.
	498	re 490: Concern on Carriers is on "Bomb Alley" for these type of issues. It will allows us to know where to place the access point. Does anyone have a status on the exact issues around this letter???
	500	Re #490 - Need to look not only at the staging areas but the path the weapons moves along as it makes its way from the magazine to the flightr deck
	520	re 498: On the T-AKE program we're working closely with NOSSA on this. The letter does not apply to magazines and ordnance assembly areas. Ordnance handling areas are different, the letter should apply there. Joe Mackes
	529	re 520: Who do we go to concerning "assembly areas" , My AO bubba's will want to know?
	533	re 529: Need to talk to Chuck Wakefield at NOSSA or Chuck Denham at Dalgren.
493		IRC = Internet Relay Chat
	495	re #493 - thanks

# Appendix H, GroupWare Comments

501		Didn't letter state less than .25milliwatt it was safe around ordnance?
	504	#501 - Believe it Stated safety limit was .22 mw -
	505	re 504, does that translate into a "distance" from ordnance?
	512	#501/504 - there was some distance - 1 or 3 meters// can't recall - maybe it was 1 meter / 3 feet..
	517	Re: 501/504/512 thought at .25mw or lower there was no distance issue?
	521	Re 517: Except no physical contact.
	526	Re 521: so WLAN and handhelds at less than .25MW would be safe to use around ordnance as long as you don't touch the ordnance?
	527	501/4/12/17- Distance is from emanation from secure sources... believe testing was for torp repair with wireless maint modules... needed to be 1/3 whatever's from the classified source.
	528	Re 526: That's how I read the letter.
	530	re#526: What's the usual power level on an AP?
	532	Re: 526/529 -Various levels available from 5mw to 100mw - depends on AP Vender
	538	re: 526 While the letter appears to read that .25 mw is a blanket approval it doesn't apply to magazine and ordnance assembly areas. NOSSA needs to approve all RF emitters in such areas regardless of the power level.
	539	Re: 538 thanks for clarification.
502		on carriers, the ships crew's chiefs berthing is immediately under the aft mess decks where the forklifts carry the bombs from one elevator to the other
509		should we be getting optevfor involved in these tech demos to do an operational assessment.....value added ?
	511	re 509: Getting OPTEVFOR involved could be messy.
	516	re 511 - OPTEVFOR has made informal inquiries about what we're doing. Hasn't gone any further than that (that I'm aware of) Wanda
	523	re 509-the test and manning areas have similar demands and there have been discussions about including them upfront and early similar to the users. Unfortunately, their organizations are small and the demand great if the early involvement is acted on. Would like their involvement early so that issues they id could be addressed and make the back end the easier vice the acid test after significant resources have been spent.
510		EMCON tests - how do you really get a good test - looking for emitted signal just at sea level? or over some hemispherical space around the ship? How to account for other parameters - atmospherics, ducts, skip, space diversity etc.
	513	re#510: or under the ship?
	515	re #510: excellent. what about capturing what I type on a wireless keyboard. not only from off ship but from another compartment.
514		pre-mature for coff. they will see technology when inserted in por
518		it would be interesting to re-poll all those folks that responded that "Cost savings" was the largest benefit to wireless (ranked #2 on the survey) given all of these additional costs that Smart ship incurred.

## Appendix H, GroupWare Comments

522		Wanda-does the netwarcom n8 conops for experimentation address the OT issue ? ghs
	536	re #522 - Glen, don't know, but I can ask the I&E FORCENet experts - Merle, CWO2 Garcia or Glen McLeod - any quick assist here? If not, got it for action. Wanda
	543	re #522 and #536 NETWARCOM recommends including OPTEVFOR as an observer in experimentation. There is an assessment OPTEVFOR does on experimental systems but I don't remember the terminology. I'll look for the information tonight. Merrill
524		Biggest concern is the time to implement at COTS solution, and if you change the arch due to an upgrade and the requirement to re-test. We seemed to get in and endless Do Loop when we just went through one of these processes, although it also contained software applications, which change more frequently.
525		On T_AKE we were surprised to hear that people thought this would be cheap. We are only using it where we absolutely have to.
531		Scott, for TEMPEST, the POC I worked with was Jim Care at SSC/CH.
534		530- got to keep both AP and hand held device within 25mw when they are "seeking" mode.
535		thanks for poc's
537		Need a list of POCs for ship integration such as HERO, EMI, RADHAZ, TEMPEST, and all the other criteria...
	562	RE #537, #545 and Ref #558: a recently signed and released SPAWARINST 3090.1 contains a pretty comprehensive list of Cross-SYSCOM POCs for HERO, EMI, RADHAZ, TEMPEST, EMC and Topside design. And within NAVSEA, Ron Bradley is the E3/SM Warrant holder for NAVSEA that encompasses all of those disciplines. Several folks are here this week that can assist further. Scott Hoschar, NAVAIR, Mike Stewart, SPAWAR, and Willie Miles, NAVSEA.
540		Does NETWARCOM have a specific POAM for coming to closure on policy and specific acquisition guidance ? With all the disjointed pilots/demos going on across the board it would be helpful to those of us providing guidance to the acquisition community to know specific milestone dates.
	547	re 540: I thought all experimentation done would be entered into the Sea Trial Information Management System (STIMS). If it is in STIMS it has CFFC visibility and is on a path to be tested in a Sea Trial experiment and make its way to a Program of Record.
	550	re 547: what is "AirFortress?"
	551	re 550: A company that sells wireless products
	556	re540 and 547-is this true for only tests labeled Sea Trials, because the tests run on the DDGs were not labeled such as far as I know. We could have used OPTEVFOR input/participation.



## Appendix H, GroupWare Comments

	563	Re: #540 NETWARCOM's role WRT WLAN's will deal specifically with the DAA/Security aspect of WLAN operations and there is an existing POA&M for our DAA functions,. NETWARCOM N6 will work the key stakeholders (FFC, PEO Ships, OPNAV, SPAWAR) to propose an overall WLAN policy/roadmap which should recommend specific "rules of the road" for the acquisition world to consider. This WLAN "roadmap" is one of the key deliverables that we want to get to as a result of this summit. KKU
	573	Re 563: When will NETWARCOM be assuming the DAA function for Navy networks? The message noted that a POAM will be forthcoming but the date for the actual assumption of DAA duties was not listed.
	575	re: 563- will this be applicable to shore activities as well ?
	576	re: 575- yes
	577	re 563: KKU, Still confused who is the single belly button. NMCI, IT-21, and MC Tactical Intranet is a nightmare for application/process owners. Can we start a dialogue to have a standard tactical network approach that covers shore and afloat, including Intermediate Maintenance and below on the Air side?
	580	re 577: and throw ERP into the acronym's as well..
	582	Re: #573: OPNAVNOTE 5230 of 2 Aug 03 appointed NETWARCOM as the single DAA for all operational Navy Information Technology (IT) systems and networks. This includes IT-21, NMCI and BLII OCONUS. So, to answer your question, NETWARCOM has already assumed the DAA functions - were now working out all the details in the POA&M for implementation, especially covering the Local DAA's responsibilities. KKU.
541		What exactly does DES stand for? Have heard double and triple DES... Thanks
542		Digital Encryption Standard
544		Double DES in not usable
545		lance, let's work up list of those in syscoms with technical authority for herp, hero, herf, emi, radhaz and tempest, ghs
546		AirFortress has a product that encrypts everything in a packet except for the source and destination MAC addresses
	552	546- Understand Cranite also meets this criteria as do other vendors, where do we turn to in Navy to "verify" this is true?
	564	Re 546 Yes, Cranite is another FIPS 140.2 approved wireless networking solution. If you go to Air Fortress tomorrow, you'll hear them bash Cranite for Cranite only approved their access system and not their client. As of last week, Air Fortress obtained certification of their client in addition to their access system. Regardless, once my Protection profiles are published, it is a mute point for they'll both need to go through Common criteria.

## Appendix H, GroupWare Comments

	566	re#564: regardless of the vendor, I like the solution. have you seen the system for PED's which allows you to encrypt the file system based on keys which are stored/served from the wired lan? if you take the pda out of the lan, you effective have a very expensive paperweight.
	567	566- good solution if you are chained to that network.. What happens when you need to use the PED outside that network, i.e. from ship to shore ?
	569	re#566: Would you want to allow that?
	578	re 566: No, I've not seen that system for PEDs. Who makes it?
	581	re 578: Cannot remember. We may see it tomorrow though.
548		To add to AES implementation for classified, NSA have requirements for high-assurance products. I can appreciate where an AES WLAN solution is cheaper than Harris Secnet-11; however, by the time a AES-implementation goes through the process to include all of our high assurance requirements, I would almost bet the cost will be comparable to Harris SecNet-11. Additionally, this approval would be for Suite B of Crypto modernization use for coalition interoperability, tactical scenarios, allied interoperability.
	554	re #548 - But....at least it would promote competition. There would be at least two qualified vendors. mmmh. ?
549		AES == Advanced Encryption Standard (Rindjael algorithm) (I can never spell that correctly)
553		Layer 3 will be the layer for the INE protocols "off ship" with the red/black separation and the HAIPE device. Why would we go with a different architecture for the shipboard LAN, is it more vulnerable than off ship architecture? Doesn't make sense.
	565	re 553, the HAIPE INEs are not wireless. Those that have implemented a wireless mode are not approved by NSA. If you do not mind paying 16K+ for a solution, then there is a wireless INE going through NSA certification
	579	re: 553, 565. HAIPE INE ????
	583	re 579. The INEs that are out there are not all compliant with HAIPE standards. I know they are trying to finalize 2.0 so most will be compliant. I say HAIPE INE to address INEs that have type1 encryption but are not HAIPE-compliant.
555		it's a "transparent" encryption product.... effectively it's a marriage between a bridge and an encryption device... because it encrypts everything except the source and destination MAC's, you have to be in the local network to be part of the VPN... you then make the conversation wireless by pushing it through an access point in bridging mode
557		Is there an established process for evaluating wireless technology for Fleet?
558		I have a list of technical POCs and NAVSEA has TA authority for most of the areas. See F. M. Stewart
559		NSA/NIST has a great web site that lists ALL FIPS-140-1/2 products - in progress and completed status...
561		application candidates should examine: eoss, ietms, personal locator, atfp,dc, rf id tags.....

## Appendix H, GroupWare Comments

568		When Marines are embarked on Navy ships will they use their wireless devices via the ISNS architecture or will they have a separate system off of the MAGTF router (which is an ADNS system and not ISNS)? Just trying to get a better handle of this platform network LAN vs. a WAN capability and how the two interface.
	571	568- MARCOR to plug into ISNS and when Ship to ship and/or shore will use ADNS.
	572	re 568: They currently use the MAGTF router when going wireless off of the ship.
570		I am not saying ever user needs a HAIPE device, even though the JTRS arch looks like that, but at least at gateways at the enclaves would need that and when the WLANs would want to go off ship.
574		Michelle McGuire USS Coronado Case Study 14:20 Monday
584		HAIPE - High Assurance Internet Protocol Encryption INE - Inline Network Encryptor
	585	re: 584 thank you.
586		ERP is Enterprise Resource Planning
587		We could use a Wiki here to keep all of these acronyms in. Build it as a custom summit-related glossary.
	589	re #587 - what's a "Wiki"?
	593	re 589: It's a web page that readers can edit. You can run authenticated or unauthenticated versions. Requires no knowledge of HTML.
	594	re 589: its an open source collaboration tool, do a google search for wikipedia
588		Everything that is NSA certified...does not necessary mean that is Joint Interoperable! A good example the STE!
	591	re 588: Do not disagree. We, NSA , do not require JTIC testing and it is something we are trying to improve upon on our products to satisfy the services.
	603	Re #591, I stand corrected, I meant Joint Interoperability Telecommunication Command (JITC) Certified.
	604	re: 603 - Thought it was Joint Interoperability Test Center
	605	re 603, I erred for I meant to put JITC, Joint Interoperability Test Center.
	618	Re # 604,605, and 611 JITC changed their name. However, I believe you are correct in part, since 'telecommunication' should be 'Test', "Command is correct, I will verify.
590		Boeing will implement HAPIE standard 1.1 for JTRS Cluster 1, unfortunately it will only pass source and destination IPs and not DSCP which the Navy and DOD expect for QoS management. So you can see the problems with system wide architectures in the WAN. HAIPE 2 and beyond will pass DSCP, but if Cluster one delivers in Fy 09 or FY 10, figure out when 2.0 will implement. If the other alternative is to do an ECP for Cluster 1, each ECP proposed has been quoted in the tens of millions of dollars.

Appendix H, GroupWare Comments

	597	Re 590: I can say HAIPE is a bandwidth hog. NSA is going through a process to understand how to define HAIPE for our low-bandwidth, low power devices: tactical radios, PED/PDAs, cellular, etc. Not sure what we will call it - HAIPE mobile, HAIPE-lite?
592		Turning off the SIPRNET WLAN during EMCON seems a bit extreme, there must be some other mitigating measures that could be instituted to allow use of the WLAN even during EMCON..RNO
	596	re 592: I can "see" setting EMCON in specific zones
	610	RE #592: I would agree. I would think that at least one goal of the EMCON test would be to assess EMCON susceptibility of the SIPRNET WLAN. I cannot believe that if this WLAN is going to be used operationally, that it would be secured during EMCON. Or is that an incorrect assumption ?
598		Harris did some freq shifters to get the SecNet 11 out of the ISM bands for ease in freq clearance so it helps in mitigation. I think they moved down to the 1.9-2.0 GHz range. It is VERY hard to get these freq cleared in WestPac.
	601	598-599 is elliptical curve still a viable algorithm under FIPS 140-1 or 2 ?
599		I have heard of HAIPE Lite for SRW since this will be the handheld waveform for Cluster 1 and they are concerned with battery consumption for handheld devices in the field. This is the proposed Type 1 handheld.
600		Dave, Michelle, will it help if I pass on to you some classified comments regarding SecNet-11 from Bill Mace, NSA TEMPEST POC and responsible for CTTAs. Bill Mace holds a bi-annual meeting with all the CTTAs. For the past three meetings, he has talked to SecNet-11. I know Jim Care has been in these meetings.
	616	re 600 - yes, please. Michele
602		a little overlap read competition is sometimes a good idea
	608	re 602 & 595: set your comment display to APPEND (it is set to "before" tsk tsk, poor etiquette)
606		There is another SecNet 11 Wireless test bed at MCTSSA at the ONR S&T test bed, it also connects to the IBGWN test bed at SSC-SD. The MCTSSA site will also connect to the STOM Bridge for BLOS extensions to the SWLAN via IMMARSAT and TACSAT (I think they now call this CONDOR).
607		RE: SIPRNET pitch from M. McGuire - EMI/EMC these are really platform related tests that would have to be conducted on each platform to assess impacts to shipboard systems.
609		Coronado testing should include ALL wireless networks (sipr and nipr)
611		JITC changed their name. However, I believe you are correct in part, since 'Telecommunication' should be 'Test', 'Command' Is correct.
612		608- if used properly the before and after helps keep comments in a "thread".
	615	re 612: ROE at the beginning of the conference said leave it on Append.
613		Glen Hoffman USS GW Start 14:45 Monday

## Appendix H, GroupWare Comments

	620	re 613: This also applies to Amphibs when the Marines show up. They bring their own computers and have the ship setup the LAN drops. The configurability and cost savings of wireless are very apparent in this situation.
623		what is the time duration "requirement" for UPS battery power (in hours) for wireless networks ?
	625	re 623: is there one?
	629	re #623: ups are not for running the system. they are implemented for having enough pwr (in time) to shutdown the system.
	630	re 623: UPS are usually measured in minutes not hours.
	631	re 629: shutdown the system properly to minimize the loss of data. measured in minutes not hours
	634	re 623: It also depends on the load on the UPS, age of batteries, etc.
	635	re 634: that is why PMS on the UPS is important
	637	re 623. This is an all depends type of question. For most of the PEO C4I installed racks, the minimum is to allow for the rack to be properly shut down. Some racks that are "mission critical" have other time lines that are not standard. Currently there is no in writing UPS requirement for racks that just support ISNS networking other than safe shutdown. See Capt Kendrick for a complete discussion.
627		I would imagine that the routing domain for the ISNS is not the same as the ADNS domain back to the NOC. Is this another problem for the Marines? Will they join the ISNS AS when they are wireless and then when they transition ashore they need to migrate to the MAGTF router? Doesn't ISNS and ADNS have a border gateway protocols running between them. It just seems a little challenging to figure out how transient organizations come aboard and get network services without configuring every device and then changing it all as they leave the ship. Probably an issue to investigate.
	644	re #627 - when aboard ships Marines will operate on the ISNS, this will require clients to be configured according to the ISNS domain. When they transition ashore, they will have to go to another domain and pass information via ADNS and the MAGTF router. Our clients ashore will have another configuration to operate an ashore WLAN. This is a HUGE issue for the Marines because we know that we have to operate in 2 different environments - ashore and afloat. We are trying to keep everything - software and hardware as close to COTS as possible and reduce the reconfiguration as much as possible. The ADNS and ISNS is not a large issue right now because we are only looking at embarkation data using these two pipelines. As the number of users and applications go up, we will have to address the different domains in the future.
632		so long as the techs can bring it back up in minutes
638		UPS standards are very specific... our shipboard UPS stated 2 yr battery life - and 5 out of 7 literally Burned up at the 23-26 month timeline! At least they had truth in advertising!

## Appendix H, GroupWare Comments

640		6-8 APs for submarines only equates to the forward end of the ship, not the engine room spaces!
641		lance-will mason test report be unclas ? ghs
	645	Re 641: Yes. We will clean up somewhat so no MAC address info and such is there for public release. But should not have anything classified.
643		Speaker just made the case for dynamic Quality of Service!
	646	re #643: wireless QoS?
	647	re 646: Yep
	649	re 647: heh...
648		WILL not have anything classified ghs
650		BMAC ain't the end-all-be-all for QoS...
	651	re 650: Agree...Every solution has it's own problems
	652	re 650: Yeah, it has a whooping 3 selectable QoS functions now (Inport, underway, and fires)...
	656	re 650 BMAC was a tool to develop QoS requirements in conjunction with Packetshaper and CISCO 36xx routers for PMW 179 in the ADNS system. We learned a lot and need to move forward from BMAC.
	657	re 652: It's all dependent upon how you set it up (I am not advocating this product cause I know there are others).....The problem is getting the QOS to work within ADNS.
	658	re 657: Here! Here!
655		BMAC is also not the only product that will do application level "QoS" marking.
659		Cisco switches can mark traffic IAW DiffServ values. On voice the MLPP was what I thought the stumbling block for VoIP implementation. It is hard in the IP world to do the "old" commander bumps the junior users of their voice traffic, not by type of traffic, but by who the user is and his/her billet.
	663	Re# 659 According to the JS-J6-T MLPP is not a requirement under the IPv6, instead 'assured services'. This statement from the JS blew everybody's mind last week. Since this is/was one of the most important Military Unique Features (MUF) the CC's (Warfighters) use for C2. I personally think is an error!
660		Walt Kostyk USS Elrod Case Study Start 1510 Monday
661		More bandwidth needed off the ship for this and many more products
	662	re 661: There is no current bandwidth requirement for non-tactical applications.
	664	re 662: You tell the ship that and also the CSG Commander
	665	re #664: agree, tell a submarine that the application eats bandwidth and it will never be used.
	666	re 664: Just stating facts...if the CSG/ESG commanders want this then they should report it as a requirement to higher.
	667	re #665: better yet, cannot be used
	668	re 666: If you look at the C2F / C3F requirements it is priority one..... Maybe more detail is needed but it is there.

Appendix H, GroupWare Comments

	669	re 668: More bandwidth is priority 1, but that is usually stated for TACTICAL applications. There is no requirement for non-tactical applications.
	670	re # 661 Reference IP requirements, The tactical entities are planning to use G729.A, bandwidth is a BIG issue in the field!
	671	re 668: agree with that also, email is not mission essential and getting it as a requirement will be next to impossible
	674	re 661/668 where do logistics and supply data requirements fall ?
	675	re 668: however, non-tactical bandwidth and tactical bandwidth still come down the same pipe, at least on a submarine it does. so one takes away from the other
	676	re 674: Non-tactical or newly dubbed Tactical-support.
	677	re 676: good one
	680	re 675: We can't continue to state that we need more bandwidth/efficient bandwidth usage unless we can state how much we need. Congress and the others who pay the bills are tired of the "we need more" mentality. We need to make the case.
	693	re #680: okay. the submarine force is transitioning from IXS (information exchange systems) to IP (internet protocol) systems. We currently do not have the capability (antenna size) or Satellite access both afloat and ashore to effectively complete this task. Basically, more satellites are needed.
672		Am I missing something, isn't the Conditioned Based Maint data staying in the most part within the ship? I don't think much of this data would have to go off the ship until it is aggregated, synthesized, and then a summary report could go off the ship to some maint facility.
	686	Re #672 that is correct this is part of a ship intranet and would only go off ship via a fire walled interface through ISNS
673		c3f/c2f did NOT SPECIFY TACTICAL bandwidth - we stated Big deck / Small deck effective throughputs
678		bandwidth is bandwidth
679		What about TFW data traversing between ships. I thought that TFW's portal dealt with some logistics databases, doesn't this traverse the off ship networks and eat BW.
	685	re 679: TFW requires a lot of bandwidth (mostly for dir replication)
681		Bandwidth is a drug. The more you get, the more you want.
	683	re 681: It is just like your salary. Your spending increases as it does.
682		bandwidth icd ?
691		How much BW does HTTP data for web portals use? Or do we have an architecture with a large number of web servers; much different than industry. I have asked TFW for this in the past, but never could get the answer.
692		How much of this "demand" for data is redundant ?

## Appendix H, GroupWare Comments

694		Re bandwidth-the bandwidth can be minimized at the device. Not all the data collected has to go out of the space until an operating threshold/ deviation is realized. Granted, if used for a large number of devices, the design philosophy has to be to control overall bandwidth rqmnts.. Since the population of sensorized equipments hasn't been developed, the business case has to built through system engineering process to define the bandwidth issue.
695		End of Case Studies Break 1522 Monday
696		C3F/C2F did the basic number crunching with support from CNA to assess current use, needs, shortfalls. Then ID'd the listed FNC's for netted sensors, ISR supported systems, Intel Feeds, GBS, etc and came up with BIG Decks: 50 MBPS / all others 25 MBPS effective throughput.
697		One thing to keep in mind. Wireless networks are not high-bandwidth pipes. While they might be able to handle 2-5 concurrent users, more than that number of bandwidth hogs seriously affects the wireless network.
706		HAIPE 2 spec for dynamic rekeying requirement
707		John Nolen Summary 1537 Monday
716		Lance Flitter Industry Brief 1542 Monday

### Day 1 and 2 Recap

MainC mt#	Ref: Cmt #	Comment
731		Day 3 0835AM Wednesday
735		Today is the day where we try to figure out how the Navy can move forward towards getting wireless network technology to the people who can use it! Let's focus and do something good for the Navy!
736		Regarding the Case Studies, I do not remember any discussion of the implementation of intrusion detection systems (IDS) such as the commercial product, Air Defense. Was an IDS installed and tested during any of the shipboard installations?
	742	re736 I also do not recall any mention of VPN Virtual Private Networks to obscure the IP addresses
	747	Re 736: I don't know of any implemented IDS but I know many people are looking at them, including Smartship. We are looking at commercial solutions and have R&D efforts developing some specific ones as well. - LAF
737		You have at least 14 users here because there's 14 active duty in the room.
	738	re 737: the EMO from the USS Mason was the only ship board active duty user of a WLAN on a Navy Ship.
	740	re 738: If WLANs are going to be used, then all active duty deplorers will be users



## Appendix H, GroupWare Comments

	741	re. 737 - No the two C3F personnel are WIRELESS users from the COR as well as some of the SPAWAR personnel.
	743	re 740: key word is "if"
	746	re 737 coming from Army, I know the lower enlisted were the actual users, the ones who had to directly operate the devices vs. the officers and senior NCOs not necessarily operating the equipment. I would question whether there are actual users in this room.
	786	re: 738. The COMTHIRDFLT J9 is in attendance as well and has a WLAN onboard USS/USNS Coronado.
739		Everything discussed and presented will by made available to all attendees including the useful portions of the Running dialogue will be captured both the raw form as a word document and will be analyzed for the final report from this conference (which will also be posted) and survey results.
744		WLAN by themselves are _____. It is what get plugged into them that increases its value. How are the handhelds, notebooks etc going to be managed so that they will be compatible with the WLAN...
	749	re 744 wireless LAN clients come in PCMCIA form. Notebooks have PCMCIA ports and handheld have PCMCIA sleeves. Some instances I've seen them come in USB format, which computing platforms come with today.
	750	Re 744: Yes, WLAN is an enabler. It's value is in how it is used.
745		Will Dr. Josts' brief be included in the material posted on the website?
	748	Re 745: Yes, Dr. Jost's brief will be on the website.
	751	Re #748 how long before the info is avail on the website
	758	Re 748: ASAP. Hopefully by next week.
	759	Re 751 - Information from the Summit is expected to be posted on the Navy Knowledge OnLine website NLT 19 Dec. Detailed info will be provided in the summary. brief.
752		Under the NAVY's policies or regulations, is a COI WLAN allowed to interoperate in a WAN environment?
	753	re: 752-- under which umbrella is the blackberry?
754		The PACOM policy is rigid, but rigid for the reasons that the developers need to answer. For those of us who are assisting in the development of this technology, bringing the understanding through testing results so that policy makers to users know the technology should be our goal. Rigid policy reflects the unknowns or knowns that reveal vulnerability.
	763	re 754: In the long run policy that is based on unknowns or is to restrictive ultimately does not accomplish its goals. In the case of PACOM, the policy may be so rigid because of the unknowns.
755		Waivers are NOT the answer.
756		however, once a command puts out a policy like PACOMM did, everyone points to that as being the standard down the road which impedes progress do the road.
	757	re #756: would you rather there be nothing in place

## Appendix H, GroupWare Comments

	762	re 756: no the point is some one puts out a policy and never cancels the policy when another one covers that same area
	768	re 762: that is a broad statement without much thought, however, a lot of emotion
760		Sounds like this is about risk analysis... Do we know what the level of risk that is okay for using wireless?
	766	Re 760: No, I don't think so. And that is one of the major things holding us back. Need to get more info to decision makers so they can do the risk analysis and make the call on operational guidelines.
761		It may not be impeding progress... it may be raising the bar higher in a specific requirement which forces vendor and developers to implement.
	764	re #761: agreed
	772	re 761, unfortunately the profit from government is small in comparison to commercial market, as I am sure you are aware. It would be difficult to convince the SMEs - CISCOs and Lucent's - to raise their bar.
	773	re 761: that is why we must
765		8100.bb is a baseline. One concern for PACOM's rigid policy is technology moving to fast, adversaries are very smart and able to purchase inexpensive hacking tools, and what one thought a product was secure changes because of obsolescence of part.
	771	re 765: This statement is true of all rapidly moving technologies. Rigid policy often results in wavers becoming the rule rather than the exception or other circumvention of policy.
767		what makes something that is unclassified into sensitive but unclassified?
	775	re 767 aggregate of information
769		As soon as detailed studies and technical security issues have been address..policies can be changed..
770		Will NETWARCOM or CFFC "recall" the CPF/CLF moratorium on Wireless - now that we have the new DAA in place? or will the Fleet N6's still be able to push their own fleet specific agendas? When can we expect to have ONE NAVY standard? WHO should be the DOD Champion for Wireless LANs? DOD CIO? JFCOM? CFFC?
	784	re #770: I was, have been, and am expecting that those heavy hitter type discussions would be the focus of this summit -
774		shouldn't we id a navy champion for each application ?
776		re the policy stream-discussion of that policy, under what context was the policy created and what was viewed as the motivator(s) is key. The Policy approvers and drafters deserve attention. Those that understand the technology (the community of experts) need to open dialogue with those policy makers.
777		Who will be leading the effort to coordinate funding resources?
778		One item I do not here is cost. In some instances, the cost of upgrading or implementing a wired network is more than a wireless network implementation.

## Appendix H, GroupWare Comments

779		The policy may have been created on the premise that with wired connections you have the physical control of the bldg spaces of which the unclass Intranet is housed. With wireless you lose that control.
	780	re #779: you don't necessarily loose control, it is a different type of control
782		When wireless security and technical issues have been addressed then PACOM may change their policy... bringing the 'control' and 'understanding' back.
	785	re 782: "may" is the keyword
783		Today, there are a number of folks with a wireless phone that do not have a wired phone in the home and the numbers are increasing. I can see the same happening with wireless networks over the next several years. Wireless networks are starting to come into the household and it will not be too long before it is common to have a WLAN in your home such as one has a microwave or a cell phone.
787		re discussion of policies, DISA's uses architecture unique policies, whereas capabilities/security or doctrine vary dependent on its network supporting role. For example a node voice switch must meet all requirements of the Generic Switch Communication Requirements (GSCR), but at the low pole, the PBX2 does not have to meet all requirements, however the PBX is strictly used for COI ONLY and MLPP is not even required....be strategic or Deployed. Maybe we can follow a similar arrangement
788		he said NMCI and "be able to use" in the same sentence
	792	re 788- and he didn't say \$\$\$\$ to be able to use. We must speak in complete thoughts.
789		In reference to the PACOM policy, they are concerned about the rapid insertion of technology and operational impact. Recommend briefing PACOM on the wireless user guide to show that the acquisition community is considering the criteria such as security, EMI, etc.
790		In terms of joint operations and big vision, how many people attending Dr. Jost's talk yesterday and how do you think the high-level vision for the GIG influence what we are trying to do here?
	796	re 790, I know from an NSA perspective, we've restructure to specifically work under this GIG umbrella. GIG will drive our requirements, etc.
	801	re 796 Also, I failed to also discussed Horizontal Fusion, which Dr Jost included in his brief. from my understanding, Horizontal Fusion is to address the rapid delivery of SIGINT from the IC community to the war fighter. I am sure there is more to it.
791		PACOM CIO has seen a demonstration and brief on wireless networks
793		Sorry for repeating but PACOM IA needs to have all the security concerns and technical issues resolved or mitigated and that will change/improve the implementation of the policies.

## Appendix H, GroupWare Comments

794		Regarding what the Army and AF are doing with WLAN, for the most part , it is being dealt as an extension of the wired network. But, in the tactical battlefield, generally it tends to be stand-alone. I know Army is using WLAN within Saddam's palaces because they can not drill into the marble columns; however, it is not tied back to the TOC (Tactical Operation Center). AF has struggle with how to deal with WLAN. I know at the AF Summit they hold every year in Aug, AF stood up and said wireless is now and we need to deal with it. There is a recognition on AF's part to deal with it. From a security standpoint, to get away from SecNet-11 proprietary nature, NSA is developing a HAIPE solution for the low-bandwidth, low power devices such as WLAN, mobile phones, PDAs, etc for high-grade security and interoperability.
	803	Re#794 The ARMY and AF are relying on the WIRED network operational and security requirement, where the wireless is placed in a gateway tier to access the wired network. They recognize that they are in a transitional period, thus build hybrid networks.
	804	re 803. Yes, I may have not made that clear; however, they are making efforts to define wireless and how it should fit into their requirements. I do not believe we'd ever get aware from wired backbone, at least for now.
	808	Re 804 and 805, DISA has a program, here in Wash DC, that focus on category/Class 5 Soft switches at to support Wireless and VoIP technology. For JUICE 04, DISA will insert four types of packet switches (Cat 5 (MFS capable)) to assess their capability and supporting requirements. Dr. Shah (Eagle Building) is the POC within DISA.
795		PACOM needs to be aware of this forum and guidance such as the warless guide that is being provided to allay PACOM concerns.
797		The PACOM policy reps were invited but had other commitments. They will be informed of the results of this meeting.
798		NMCI is not a panacea unless you have really deep pockets.
799		Dr. Jost's brief has a major impact on this group. If you do not meet the security requirements, the distributed services and application standards and so on, then no funding can be applied to that program...
800		are the submarine WLANs IPv6 compatible
802		I agree about Dr. Jost's brief. The level of seamless interoperability and incredible depth of access within the enterprise requires a different way of thinking.

## Applications and Capabilities

MainC mt#	Ref: Cmt #	Comment
805		If you develop applications based on web services then the wireless and wired network layer is abstracted away.
	807	re 805, True, the application layer is separate from the network layer.
	825	re 805: Understanding webservices, what about content...i.e., IETM's for HM&E and possibly training material? How do we know what standard to build content too?
	832	re 805 and 825- build it as thin as technology will allow
806		The ships and fleet units available for testing and evaluation must be sched through the Sea Trial process and the best POC's are the C2F and C3F staffs, as well as the TYCOM's.
809		Does NMCI fit into the GIG architecture or will Navy have to "spin" it to fit.
810		Why do we have the "Sea Trial" experimentation process if we don't use it on these types of projects?
	816	re 810 What or which Sea Trial process? It is being rewritten. Also the CNO told NETWARCOM not to wait for the Sea Trial process and move ahead. And what has the Sea Trial effort produced to date beside having many meetings? Final note, is wireless technology still an experiment or deployment of developed capability?
811		Requirements and issues discussed so far address permanent types of WLAN's. Would issues be different for a temp type WLAN that might be utilized by damage control personnel to cover damaged areas of a ship?
	812	re #811: temp for testing or for implementation
	813	Re 811: That would not be a tmp WLAN, it would be a permanent WLAN that is only used occasionally. But there are special issues such as use in smoky and electrically charged environments.
	818	re 811: As far as temp installs they have to follow the same process as a permanent installation (ILS, drawings, etc...)
814		NMCI fits if you view NMCI only providing the network services
	817	re 814: They just don't provide in quality in the network service
815		Regarding GIG architecture and interoperability, does anyone know if any of these wireless LAN standards or IEEE protocols are included in the Joint Technical Architecture 4.0 or 5.0 or whatever is the latest version of JTA. The JTA is the basis of the GIG architecture.
819		Quality could be abstracted higher in the application/enterprise tier.
	820	re 819: explain
821		Quality of service can be implemented via enterprise business rules access lower layer network resources. It may not provide the detailed network layer QoS.

Appendix H, GroupWare Comments

822		What about devices? Is there an anticipated standard for the wireless device?
	824	re 822 in some instance devices comply with 802.11 and other instances 802.15 (bluetooth). Two standards that are suppose to coexist but no interoperate.
	827	re 824: Are we to assume that any compliant device will be allowed?
	834	re 827, from a security stand-point, no
	844	re 824, CECOM is assessing a wireless soft switch that may permits such interoperability. It allows CDMA, GSM (800-1900), 2.4 and .58 to interoperate (VOICE).
	847	re 844, the problems I have seen in this wireless software switches is (lack of) connectivity to the commercial network. If you do not care about relaying back to your higher, then it is not an issue.
	849	re 824,844 Motorola, and Phillips are releasing new set of chips that permit both 802.11 and GSM/GPRS so that when in range of WLAN or hotspot inside home "tool" would use VoIP when leaving the "home" it would automatically sync to the cellular "lines"... Convergence is happening very rapidly.
	852	re # 847 our assessment shows that a media gateway (4 to 16 ports) in combination with a Softswitch will simultaneously and successfully connect to T-1/E-1 MFr1, DTMF, PRI (ISDN) or fractional T-1 to the Teleport/STEP sites. In fact, we were able to make end to end secure connection with Type 1 encryption.
	855	re 852,True and I've seen it, but an example comes to mind with Guantanamo Bay. The have an issue with that fact that they are not tied into the commercial cellular infrastructure and that is a major issue as far as they are concerned.
	877	Re #855 we are working several solutions for the GB issue, this is not a technical problem, but a policy problem. One potential solution can make the GB switch look just like a Post camp switch extension and configure it to has 'Class A' authorization as long as DISA permits it.
823		re Sea Trials-consideration is being given to aggregating and testing networked technology projects during a sea trial ...wireless lan, c-band antenna (for small ships) distance support and testing those. This was discussed at a Trident Warrior exercise mtg and Merrill Witzel mentioned it in the FORCEnet brief. Whether that occurs is at risk, but the approach is the right direction. Now to get some \$\$\$, reduce the risk and show the possibility and effectiveness of the approach.
	826	re 823: Looks like we can discuss this at the next TW04 meeting.....
	829	re 823: TW funding is a huge issue
828		We need to ensure that wireless standards identified in forums such as this are the JTA but not all per the discussions today. Standards are in the JTA but not all.
833		Expert communities, users and policies will help develop XML standards for your content. Business rules and services will extend from there.
835		Is there a quick explanation of difference between 802.11 and 802.15 ?

## Appendix H, GroupWare Comments

	836	re 835: 0.04
837		John Nolen Wireless Capabilities 1015 Wednesday
838		On wireless networks being an extension of wired nets or a new capability on their own -- they are both. We are all probably familiar with ways that they are extensions of wired networks but may not be as familiar with ways that they can be stand-alone. One example of how they can stand on their own occurs when you have saturation of a physical space that are wireless capable. If they can all switch to a peer-to-peer wireless mode, then you don't even have to have any wired infrastructure to support communications and applications -- ad-hoc wireless routing algorithms can enable you to form a fully functioning network out of mobile/wireless nodes. Any application that can be supported by a wired network can be supported by a wireless ad-hoc network....although at lower quality of service because of limited bandwidth right now.
	854	re 838: Ad-hoc wireless networks provide significant survivability benefits if all critical applications can operate on both a wired network and an ad-hoc wireless network. Normal mode is to run in the wired environment; emergency mode can operate in a wireless ad-hoc mode if that is all that is available because the wired infrastructure has been blown away
	856	Re: 854 Same thought as #811
	861	re 854 as long as you accept the security risk with running an ad-hoc network.
	862	Re 861: Making ad-hoc secure and reliable is going to be one of the most important development areas in wireless networking in the next several years.
	866	re 862-861 Anyone know how the Army has solved this in their operations ?
	868	Re: 856 The key to making wireless networks useful for survivability is ensuring that the deployed access points (any that survive) and devices all support and have installed distributed routing algorithms like DSR that enable any device to find any other device in an efficient fashion.
	870	Re 868: Easy to say.
	872	re 866, a \$16000+ per device piece of equipment from Northrop Grumman
	875	re 872: where can I get more info on this ? Its my understanding they were using Qualcomm and CDMA...
	878	Re: 870: Everything is easy to say!
	886	re 875 Army developed a standalone base station for the use of Qualcomm's QSec-800 (secure Type 1 cell phone) for voice, data comms. They are upgrading it to the 3 G standard to interoperate with the follow-on phone, QSec-2700. For wireless networking, the Army has the VRC-106, which still needs to be certified by NSA. If you go back to earlier comments, it is developed by Northrop Grumman and starting at a cost of \$16000 +. Ed Erskine, CECOM, is the POC for the work on stand-alone base stations and I can not recall the name of the gentleman at CECOM working on the VRC-106. You can call me (Anna) on 410-854-7005 if you wish to obtain their names or get more information on these products.

Appendix H, GroupWare Comments

839		Regarding door prize, to get your name in you must initial the sign in sheet out front in the DAY 3 column. I see maybe a dozen signed in there. There are more people here than that. We will generate the list of potential winners from that day 3 list. Go back and make sure you are checked off for day 3 if you want a chance to win!!
	842	re 839: for those of us that are already signed up for today, we would appreciate that no one else sign up.
840		802.11 is local area and 802.15 is personal area (bluetooth). Bluetooth would be used for your mouse to talk to your laptop and 802.11 is roughly equivalent to Ethernet. (overly simplified...)
840		802.11 is local area and 802.15 is personal area (bluetooth). Bluetooth would be used for your mouse to talk to your laptop and 802.11 is roughly equivalent to Ethernet. (overly simplified...)
841		Metrics for speed and operational range include BER and QOS?
846		Any reason the NAVY is not experimenting with wireless spectrum in the GSM/CDMA area?
	848	re #846 - it is almost impossible to specify all different standard for wireless and try to get them to be a Navy REQUIREMENT... we should NOT be doing technology for technologies sake.... What is the REQUIREMENT for CDMA/GSM/802.11 series??? It has taken over 4 years just to get the NAVY to even consider 802.11b!
	850	re 848: the point is that we (NAVY) are considering .11b, however long it took
	851	re 848, the reality is it is all migrating into one appliance. For example, commercial cellular providers are using 802.11 as an extension of the network into areas without infrastructure. T-Mobile hotspots in Starbucks come to mind?
	853	re #846: Infrastructure cost is huge for GSM/CDMA. DoD will continue to have their hands tied with what's available from commercial providers such as ATT. During such crisis such as 9-11, DoD will have equal access to the network as anyone else.
	860	re 853, Have you heard of priority service through DISA? Though, one problem with priority service is the FCC does not allow for preemption; however, you are next in line along with the other 99 personnel with priority service.
	863	re # 853 - reality check - if this discussion is for shipboard ops.... once you get 1/2 mile off shore - there is NO CDMA/GSM... do we spend \$100Ks in testing for a "nice to have" system?
	867	re 863, not too familiar with Navy operations, is there a requirement for tying into the local infrastructure?
	876	863 - CELL Phone technology only works in URBAN areas - they do not provide coverage once you leave the pier (or even in at the piers in the some areas) -
	895	re 876 - I got great coverage at sea on my cell phone in Japan...even three days before we pulled in...or days after we pulled out.....many miles out to sea.



Appendix H, GroupWare Comments

	898	re 895: You're not supposed to use your personal cell while underway...
	906	re 863: not exactly true... coverage is available in rural areas also... some phone companies have recognized that cell phone technology is cheaper than paying for 20 miles of wire for 30 customers
	916	re 898...And there aren't supposed to be wireless lans out there in some places...but there are because we have been dragging our feet in finding real solutions to these issues...people will do what they can get away with until we either enforce the rules or provide a real technical solution to the issue.
	931	Re# 895 GSM spectrum has a coverage, depending of terrain or manmade features among others, of 2 miles to 5 miles.
858		Army did field test summer 02 of a wireless maintenance activity at Ft. Bragg, understand they stood up the wireless ops in about 45 minutes, and almost 20 hours later the wired folks were just finishing up. There was also a large difference between the manpower required in both roll outs.
	859	re 858: That is a good data point!
864		This summit is for NAVAL systems, not just Navy. That means Marines / land based too.
869		Security will always be one of our top priority (if not the top). When 802.11i is out it will mitigate some of the concerns between the client and access point.
871		We cannot operate in spectrum used by CDM/GSM commercial services in CONUS or foreign
	908	re 871, currently GSm and CDMA used throughout the AF and Army are standalone with the capability to access any gateway to the Tier 01, 1 or 2, via lines, VSATS or even DSO drops.
	923	re 908- GSM/CDMA wireless also ,via a media gateway, access NIPR or SIPRnet VioP phones.
	946	RE#871: and the discussion on CDMA/GSM and the Navy use of these devices, all of this falls under the issues of licensed versus unlicensed equipment. Typically GSM/GPRS and CDMA type systems are the ones that the commercial industry has developed and is marketing as the licensed infrastructure supporting cell phones, pagers, wireless PDAs etc. The Navy, and any other Federal agency, CANNOT be licensed to operate systems in this spectrum, but we can be an "end user" and operate in this spectrum by using the phones, PDAs etc as a subscriber to the commercial service. But we cannot own and operate the infrastructure ... i.e. you can consider this the 'licensed' part. They operate in spectrum separate from the spectrum set aside specifically for wireless devices that we are discussing this week because the FCC and the commercial industry does not want them in the same spectrum. With unlicensed wireless however, there are no restrictions on usage of infrastructure (hubs, servers, access points etc) and/or the mobile units. The entire 'system' is part of the wireless package.

Appendix H, GroupWare Comments

	973	re 946, For Conus...DoD has allocated certain spectrum slice that supports the GSM functioning environment (1900's range) also the 400 and 450 range is also coming back to the DoD. We have a test spectrum slice the commercial world cannot touch. For OCONUS, in the KOSOVO area the frequency authorization was resolved like any other radio system the services have today, through Host Nation or, remote areas, by spectrum sniffing applications.
	988	RE 973: Additional detail on my #946 comment. There are GSM applications elsewhere in the spectrum, I was not trying to be too specific. But you are correct. However, the 1900 MHz band (roughly 1910-1930 MHz) is not DOD spectrum. it is still FCC spectrum that has been set aside for unlicensed applications similar to those that are licensed and that is how the DOD is using the 1900 MHz band. The DOD has not allocated any of this spectrum since it is not ours to allocate. And the 400-450 MHz band never left the DOD, it has been and will continue to be a military frequency band. But the concern here is that military also has many, many mobile and shipboard high power radar systems in this part of the spectrum. compatible operations with these existing and PRIMARY systems needs to be considered.  I agree completely with your comments on the KOSOVO authorizations.
	1066	re 988- Correct, the spectrum/frequency request procedures in time do funnel its way to the top (Beyond DoD), however regional frequencies entities, do provide specificity within its geographical responsibility (deconfliction, priority...etc...). Within DoD entities, availability and assignment of these allocation or segment of frequencies can be assign by the local frequency authority. DoD may not own these unlicensed frequencies, but they have provided guidance within DoD as to where to use them. I agree with you about the 400's segment, however my intention was to elude the fact that the GSM will be allowed to function within this spectrum, thus adding more frequencies for this specific application. I agree that some sort of management must be performed in order to designate or distribute spectrum to this new wireless initiative.
873		Note: Add interoperability and supportability to capabilities concerns.
	888	RE: #873: Also add compatibility to the list of concerns for capabilities unless the issues of compatibility and/or interference and susceptibility is aligned under interoperability or supportability.
874		One item I believe is important and have not heard is training. Again, not being from Navy, is this an assumption?
	879	re874 - training is required and training guides have been developed. Should be put in the "database" for others to use.
	880	Re 874: in addition to training how will changes to the instructions be made to use wireless tools? Both maintenance and logistics...
	884	ref 874 - If it ever gets transitioned, for C4I, it would be implemented within the ISNS training.

## Appendix H, GroupWare Comments

881		How do we implement the wireless equipment into our maintenance schools that are even farther behind the power curve with reference to current wired equipment.
	885	re 881: Naval Personal Development Command is current working in Great Lakes to facilitate wireless devices and training delivery.
882		The delivery of the training content or the technical content could be an issue if the wireless device isn't somewhat standardized.
883		Again, the school houses are years behind on what is out in the fleet.....YEARS!!!
	887	re 883- yet the academies have gone wireless on their campuses...
	889	re 887: Just because the academies are wireless doesn't mean they are graduating officers that understand implementation of wireless
	900	re 889- do you think the new officers will not ask how can they link up their wireless laptops to the ships network???
	901	re 889: Correct, but these officers are using wireless technology to learn. When they arrive in the fleet, the fleet is behind the power curve and the officer is pushed back to a paper world.
	905	re 901: True but that has always been the case. When I came in from the academy I was used to having a LAN and email. My first ship had neither.
	912	Re 901: But, these officers will be the catalysts for change... With their embracing the technology and seeing how useful it was for research and communications, they will be the driving force behind implementing (demanding) WLAN in the fleet. Remember, not only junior officers are exposed to WLAN. Both midgrade and senior officers are using WLAN at NPS and NWC.
	914	re 889: You do realize that many of the computer screens in combat are still black/green vector graphics...how old is that?
	918	re #914; do they work...
	920	re 912, if it matters, West Point was outfitted with WLAN through out the whole campus several years ago. The point is new officers are use to - in certain cases spoiled by - the technology
890		You could require SSL enabling of all network traffic via Web Services then the security requirement at the network layer could be less.
891		keep in mind that the way ahead for training is to get it out of the schoolhouses and down to the ship. this will help facilitate the users training on the equipment they will be working on; not what is in the schoolhouses
	897	re #891: you are assuming that the schoolhouses have the equipment in the first place, they don't!!!
	903	re 897:hence the push to get it down to the ship!
	909	re #903: oh, put it out to the fleet without technical support, good idea
	911	re 897: Ah, but times, they are a changing!
892		re "ruggedization, the survivability of the network is different from the ruggedness of the pda

## Appendix H, GroupWare Comments

893		Moving the security piece at the application layer may ease IA mandate on the network layer.
	907	re 893, that would be easy; however, you need to provide some level of security in both layer 3 and layer 2. Realize, security at Layer 2 would provide a proprietary solution. Without this security, you are subject to all sorts of known and well-executed layer 2 and layer 3 attacks.
894		SSL isn't necessarily secure
896		SSL not secure???
	904	re 896: I've read some articles that there are ways to get around SSL, forgot the details though..
	917	re 904: the exploits for SSL are usually through holes in the implementation... have seen command line access gained through a buffer overflow in SSL (on Microsoft and *nix)

### Technology Transfer

MainC mt#	Ref: Cmt #	Comment
899		John Nolen Technology Insertion 1045 Wednesday
902		buoy mounted repeater in soj ?
910		Based on our e-Commerce and Internet... SSL is all we have
913		Layer 2 versus layer 3 - is there a quick explanation ? Thanks.
	922	re 913: layer 2 is the datagram layer.... usually involves one device talking to another via a local piece of wire (uses MAC addresses)
	924	re 913: layer 3 is the network layer... involves one device talking to another via numerous pieces of wire (uses IP addresses)
	927	re 913: INE's are capable of encrypting at the layer three level so that even the IP's involved are hidden... normally a proprietary solution... requires specific capabilities of the access point and client software
	932	re 922, to add to it is also a question of sprinkling security on top of it (layer 3) or baking it in (layer 2)
	935	re 927 HAIPE addresses the proprietary nature by establishing common standards

## Appendix H, GroupWare Comments

	960	<p>re 913: Type One layer two bulk encryption encrypts everything. All you get is mixed up 1s and 0s unless you have the correct Type 1 Key and proper encryption.</p> <p>What the commercial world is calling layer two encryption encrypts the layer 3 (IP Layer) data and the MAC Headers are in the clear.</p> <p>Layer 3 encryption the MAC and IP headers are in the clear everything else is encrypted Unless.....</p> <p>If you are using IPSEC in Tunnel mode the original IP header and Payload is encrypted Unless...</p> <p>You are using L2TP over IPSec....</p> <p>In most cases the difference is minor and there are pros and cons to both from a security, interoperability and maintenance perspective.</p> <p>The bottom line is that unless you do a full fledged risk analysis, consider the given environment, etc. the discussion of layer 2 vs. layer 3 encryption misses some important considerations .</p>
	968	Re 913: Not completely true. There are different layer two encryption solutions. Some encrypt all of layer two, some encrypt part and some only encrypt layer 3 as you say. Depends on the individual application.
	987	Re: 968: True - The point being there are differences between the way these can be implemented and the answer is not necessarily a one simple answer that fits all.
915		Using SSL, PKI at least the content is encrypted. But the network header info isn't however.
919		re: training: Admins do need to be trained in the fine points of wireless. To users, it shouldn't seem radically different from the web enabled, game playing, sms-sending cell phones they probably already own. Also, most laptops you buy today have embedded wireless and many may have already used it in Starbucks!
921		Going wireless and the level of security is almost an oxymoron. Data still has to be human readable....
	929	re 921: I wonder if we just put too much emphasis on wireless security on the unclas side
	933	re 929: I don't
	934	re 933 I second that!!
	936	re 929: so its okay for someone to hack my unclas system because we don't secure it
	937	re 933 and 934: I meant compared to the security requirements we have on the wired side...i.e. if your wired side is less secure it can be exploited
	939	re 936: no its no ok to hack the unclas side but it probably happens
	942	re #937: apples and oranges. wireless needs the same physical security
	944	re 942: I disagree...people that can exploit your network will take the easiest path
	945	re: 921 and 923: Thanks for the primer. One more: MAC?

## Appendix H, GroupWare Comments

	948	re 937: wired side is usually very insecure as a whole... security is usually provided at the perimeter... it's the reason why >50% of incidents involve insiders (I think a recent industry survey stated that the insider problem was up around 80%)
	950	re #948: even more reason for the need for security on wireless
	951	re 945: Machine Address Code.... a series of hexadecimal numbers... the first half of which are assigned to specific manufacturers
	952	re 929: I would contend that we aren't saying don't secure it, but perhaps we can use best commercial practices that allow us to use commercial products. Ideally, emerging 802.11i plus a PKI infrastructure would provide sufficient security.
	956	re 950: agreed
	961	re 942 do not disagree but we understand wired implementation and the physical solutions (filtering power lines, firewall, etc) you can put in place. with wireless, the range of interception is beyond that of wired and we need to understand how to deal with it.
925		Even with the all technologists here in this room, I'm seeing a culture shift trying to happen that has tough opposition.
	926	re #925: explain
	947	re 926: Comment 920. Folks able to utilized new technology are spoiled?!
930		Understand that Smartship, CFFC and NNWC have put the contractor through a rigorous requirement process for their devices. That is the standard. It is also intended that those entities will demand the same standards for ILS, etc. so that the technology is acquirable. That is an overarching strategy for this technology and within Smartship S&T.
938		Wired side we have physical security!!
940		has the dust settled yet on whether ordnance is going to be class or unclas ?
941		As the saying goes, a chain is only as strong as it's weakest link
943		re security and policy, should there also be a separation from CONUS and OCONUS
949		OCONUS issues need to address Host Nation agreements and frequency uses... don't want to open all garage doors anymore.
953		I thought MAC was Medium Access Control
	957	re #953: depends on what part of computer terminology you are using, it means both
	958	re 953: For networks, MAC is Medium Access Control
	959	re 958: for NMCI, it's Move/Add/Change
	964	re 959: And those will cost you.
954		Not to say cost is comparable to gots in price, but, aside from procuring the clients and access point, also consider all the other equipment one needs to procure for security (VPN, IDS) before saying COTS is extremely cheap compared to GOTS. Also, the cost of NIAP certification is reflected in their price so is the cost comparison with the COTS products of those FIPS 140-2 and EAL certified?.
955		I thought MAC was a buger at McDonalds.

## Appendix H, GroupWare Comments

962		In any case, MAC is like IP only MAC is hardware dependent. It is how routing gets done down close to the hardware.
963		Instead of the old definitions of unclas, sensitive but unclas and the others, would tactical support and tactical data be more appropriate both deserving a handling category within a military context
965		what pub defines sensitive but unclassified?
	967	re #965: for what medium
	971	re 967: shouldn't matter...its the data that's classified
966		I dislike using wireless to provide any function that is considered mission critical in any manner... because of the inherent vulnerabilities in any form of radio communication, it would make that mission critical function very vulnerable to low-tech attacks.
	969	re #966: are you referring to shipboard or ashore
970		The real definition of NIPRNET is "non-classified but sensitive IP router network".....
972		how does data get a classification? is there a judgment on aggregation? Would think the Operational Commanders have perspective and the Threat Measurers have their judgments.
	975	re 972: why did we loose infrared on handhelds? How close would you have to be in order to access that "stream" of data ?
974		concerning "security nazi" ... as a network security type, you can call me all the names that you want as long as the network is operating securely. if you're the one that believes the rules don't apply to you, you and I are going to develop a first-name basis relationship
976		CONFIDENTIAL - any information that may cause damage to National Security SECRET - any information that may cause serious damage to National Security TOP SECRET - any information that may cause grave damage to National Security
	978	re 976: what about SBU?
	979	re 976-- what is the definition of National Security ?
	928	re 981: Yes, but the point is that ship technology doesn't keep pace with academic technology.
981		Sensitive but unclassified
	983	re 981: what constitutes sbu?
	984	re 983: usually privacy act information or propriety information
	990	re 984: thanks, since my social security number is privacy act protected, if I read my leave earning statement at home on a wireless network, do I need type I encryption if I work in the PACOM AOR?
	991	re #990: are you on a wireless network?
	992	re 991: yes
	993	re 990: The PACOM instruction was written when there was no other guidelines. Anyone here from PACOM that can suggest a revision to the proper people?

# Appendix H, GroupWare Comments

	995	re #992: yes, if you are in the PACOMM AOR
	997	re 991: Many people have wireless networks at home. With web-enabled NKO, Navy On-line, etc. much of the privacy act data can be accessed from home.
	998	re 997: my point exactly
	999	re 995: I guess the cost of my wireless home LAN just went way up.
	1004	re 991: current guidelines (NMCI mostly) require the home user to not have wireless enabled when accessing OWA
	1007	re 1004: how do you enforce that?
	1011	re 1007: (heh) Honor system!!!
982		"security nazi" is right up there with "self-imposed denial of service".... infocon delta is just that... should conditions every get to the point where you have to operate without the network, you have to be prepared for it. which is why we practice for infocon's. yet at every infocon planning conference we've attended, we have to have the argument about "self-imposed denial of service", regardless that DoD/DON instruction states exactly what the conditions are
986		Just because you have a clearance up to SECRET, doesn't mean you can look at all SECRET.....Need To Know ring a bell. Security measures are needed for all classifications Unclas to SCI
989		During the mid 90's when there were no accreditation processes for secure web sites, , I went to Software Engineering Institute (SEI) for risk assessment report for SBU data on the web. Their report was interesting - they considered risk level was primarily dependent on the amount of time data is exposed not the content of the data, i.e. during transport should be looked at different vice a database.
994		For a great site for info/research/training in security, please visit the web pages for the Center for Education and Research in Information Assurance and Security at <a href="http://www.cerias.purdue.edu">http://www.cerias.purdue.edu</a> . It was designated an NSA Center of Excellence for education in security.
996		I hear COTS and unsecure in the same breathe and I do not disagree. But, a pure COTS WLANs can be made somewhat secure by training and policy, such as shutting off broadcast mode on a AP, restricting access to a set of IP address, deploying a IDS and a VPN, use of a FIPS-140 solution, string key update policy, use of PKI, etc. .
	1008	re: 996: There are a number of FIPS Validated COTS WLAN solutions at use today within the DOD that meet the pending Commercial Wireless Policy 8100.bb.
	1021	re 1008, yes but FIPS 140 is only one piece of the security puzzle All it states is the product implemented AES correctly.. FIPS does not address, TEMPEST, MAC address filtering, assurance in the software, etc. 8500 will require those FIPS 140 solutions to meet a basic assurance protection profile recently submitted to NIAP for acceptance.
1000		Wireless is not C2 approved
1000		Wireless is not C2 approved
	1003	re1000: c2??



## Appendix H, GroupWare Comments

	1006	re 1000- DMS is not C2 approve either
	1010	re 1003 command and control
1001		its your choice to have wireless at home
	1012	re 1001: Correct, but reading the discussion thread here, it would seem that PACOM would want me to have Type 1 encryption on my home WLAN so that sensitive info doesn't leak out.
	1017	re 1012: Unless you're in (or connecting to) PACOM's domain, requirements are FIPS-140 vice Type 1 compliance
	1022	re 1012: It would be absurd (obviously) to have to use type one for the home use when the traffic has already traversed the internet via a VPN or SSL. (NON Type 1) I agree that someone should take this issue forward to PAYCOM.
1002		type I encryption for all of my friends
1009		c2 is a set of guidelines for LAN
	1013	re 1009: I thought c2 went away?
	1015	re #1013: no
	1019	re 1015: isn't c2 from the orange book?
1014		Anyway, My pay i.e..... LES... is not originated in PAC AOR
	1016	re 1014: but its delivered there
1018		PACOM is probably thinking about unclass as their unclass INTRANET not INTERNET. That's why they probably created the 'blanket' policy. The INTERNET is something else. NKO is probably in a DMZ where it is protected via firewalls allowing only SSL in. Layered Defense is required!!!
1024		Another thing to remember is that any policy produced by Navy is going to be a baseline policy. Organizations will always have the option to demand higher standards within their own domains.
1025		we need to id what we can stop doing as cost avoidance measures with companion policy changes
1026		Again back to the point with layered defense possible if the implementation provided SSL, PKI at the application layer possibly the network Type 1 requirement could be removed??? maybe???
	1028	re 1026, nope. I can say SSL, WEP are breakable. PKI only provides authentication of the user. You still have to deal with the integrity, confidentiality and non-repudiation of the data.
	1034	re 1028 I agree with you as well...I just thought possibly is some cases and waiver could apply. As for integrity, conf, and non-repud this is done at the application layer.
	1036	re 1028: all encryption is breakable at one point or another.... mostly it depends on the implementation of the algorithm rather than the algorithm itself... use of SSL, TLS, or PKI is acceptable for certain applications....
	1049	re 1036 and that is a risk decision to be made by the DAA
1027		How do we find the ROI for a wireless solution with the cost of meeting "security"...

## Appendix H, GroupWare Comments

	1032	re 1027, not being sarcastic, but is there an instance where security was cheap? If yes, was it "good enough".
	1035	#1027 - Industry has some great white papers on their ROI - that include their security measures... With the installation, training and hardware costs ROI coming in at 20-1 up to 100- 1 (or paid for itself in 90 days... etc) we can get a general feel for these factors. The other piece of the puzzle that the NAVY has is the EMCOM consideration... If we finally get the official policy / test requirements - then we can quantify this portion.
1029		I don't think that anyone here believes that PACs solution is all encompassing, however, there are procedures for updating policies that are currently in place and complaining about the fact that you have to overcome that hurdle and not producing a solution to the problem is not solving anything
1030		based on existing instruction, type 1 is only a requirement for classified networks.... current draft instruction for encryption on unclass networks is fips 140
	1031	re #1030: unclas is a classification
	1044	re 1031: okay... substitute "Secret" for "classified" in #1030. geez!
	1045	re 1030. Yes, and to add to it I can say NSA is getting involved with Homeland security. For example, the STE KOV14 card is being redesigned to encompass Homeland Security "modes". I can not honestly say if Homeland security's solution is purely a FIPS 140 solution or a hybrid between FIPS 140 and NSA encryption.
	1055	re #1044: ah, but it does say classified. it doesn't specify
1038		turning off the networks is the only way to secure the network...everything else is risk mitigation:)
	1039	re 1038: this is true for all networks not just wireless.
	1040	re #1038 agree
	1041	Re 1038: That is totally true and should be kept in mind when discussing security.
	1043	re 1038: Good one. We always say in aviation if Safety was our number one mission, we'd never fly. If security is the number one mission then shut the network down.
	1046	re #1043: not no. 1 mission, just no. 1 concern
	1047	re 1043: well said
	1048	re: 1038 & 1043 - there is always an considerations of mission objectives and how security can enable or hinder the accomplishment of the mission.
	1050	re 1043: but secure communications is a "mission"
	1051	re1050: secure communications Support the mission
	1053	re 1051: depends on the organization.... nctams mission is to provide secure communications

## Appendix H, GroupWare Comments

1042		The reason we are roadmapping -- and including technology evolution in the roadmap -- is to enable us to solve this problem of constantly changing technology. We need strong connections to standards bodies and companies to see what is coming down the pike.
1052		Some humor -- if we keep changing things fast enough we won't have to worry about security because the hackers won't be able to keep up. It took three weeks for hackers to exploit publicly announced flaws in USoft products.
1056		I foresee a "matrix" for security requirements.... shipboard installation vs. shore... standalone network vs. hybrid network....
	1058	re 1056: Almost a Matrix Revolutions
1057		In other words, different protection profiles...
	1062	re 1057: basically... for general purpose shore wireless, I'd like to see something like AirMagnet's permanent sensors installed.... our wired networks have IDS's which watch for specific attacks.... wireless networks need IDS capabilities which include ability to watch for attacks which are wireless network specific.
	1067	re 1062. To add to it, I'll just say there is not a really good IDS today. They are easy to by pass. A simple known attack is given an IDSs known scanning frequency you can circumvent being detected.
	1068	re 1067: and most commercial IDS's only include 200 or so canned signatures.... you have to go to something like SourceFire to get the higher capability and that requires hiring very expensive administrators to run those systems
	1069	re 1067: again, you get what you pay for
	1070	re 1067: It depend on if the type of IDS is signature based or behavioral .....But still you see a lot of false positives
	1071	re #1068, and how would you get those people out to sea
	1072	re 1068 again, given what needs to be employed for a somewhat secure COTS unclassified solution, is it really that cheap?
	1082	re 1070: numerous false positives/negatives indicate a need for "tuning"... nmci constantly argues against hiring the people required to properly manage their ids believing that the government should form a committee to help configure the boxes with a universal signature set.... they ignore the fact that each sensor requires tuning to the specific network
	1099	re:1062 Yes, an IDS should be required in a wireless network. However, this wireless IDS needs connect to our current shipboard IDS system afloat (RealSecure).
1059		Invert the matrix if it is nonsingular.

**Test and Evaluation**

MainC mt#	Ref: Cmt #	Comment
1060		John Nolen Opportunities for Test and Evaluation 1140 Wednesday
1063		The matrix is a good idea. Perhaps by defining environments (SBU, NIPR, SIPRNET, ETC.) and correlating them to security requirements - EAL 1???, FIPS - 140 or type 1?
	1064	re 1063: agree... (scribbling...)
1065		In the end all of these requirements have to be put into "contract language", and that means clearly stating requirements. When Navy WLAN instruction is signed out the matrix in there would be our "requirements", would these also satisfy the requirements for "hand holds" or wearables ?
1073		Navy ships use the IA tool kit which includes SNORT
1074		You know what I'd like to see at one of these conferences...they lock the doors and say, you're not leaving until we figure out this policy. Do you think we would get it done and move forward or waste away in the room debating finer points. Let's set the policy and then adjust it to meet threats as they arise...have we not learned anything from Microsoft...
	1076	re 1087; take a "SNORT" once or twice a day ??? what is this ?
	1080	re #1074: you fail to realize that we are not here to set policy
	1081	re 1074: There really aren't any policy makers here...
	1083	re 1080: oh but we are (policy makers are present) (taking notes)
	1086	re 1080: still not the intent of this forum
	1087	re 1081: NNWC has at least 3 people here
	1088	re 1083: So are the policy makers going to make a workable policy?
	1091	re 1087: No NNWC policy makers are here
	1093	re 1088 it is passive
	1095	re 1091: are you sure?
	1096	RE 1080: I thought in the message announcing this conference it said to send someone with the ability to make decisions on behalf of your respective command?
	1097	re 1095 <Looking around> Yes
	1098	Re 1097: Where do you think CDR Voter at the front table is from?
	1100	re 1097: and Captain Uhrich was?
	1102	re 1098: NETWARCOM
	1105	re 1100: CAPT Uhrich isn't here
	1110	re 1088: From a policy perspective - There are a number of us here who have had direct input into the OSD Wireless Policy and expect to influence others. We should address the big issues
	1112	re 1110: same for NETWARCOM
	1116	re 1110: Input/influence does not make a policy maker

## Appendix H, GroupWare Comments

	1122	re: 1116: but is does often make policy..... The bottom line is there is work from many angles that must take place.....We have many of the correct people in this room to do so...
1075		SNORT???
	1078	re 1075: open source IDS
	1085	re 1075 SNORT is one of many hacking tools developed by network geeks. The yearly Black Hat Conference and DEFCON is an excellent conference to understand the latest and greatest hacking tools. Realize, thought, it is those hackers who wear the white hat.
	1089	re 1085: how is Snort a hacking tool?
	1094	re 1085: I went to DEFCON this year, great learning experience...of course I wouldn't bring a wireless device there:)
	1104	re 1094 Do you know there is a Federal Black Hat/DEFCON they are now holding? NSA has a thread
	1107	re 1104: when is the next one?
	1109	re 1104: break or meeting, please specify
	1111	re 1109: Fed Black Hat/DEFCON
	1113	re 1107. Assuming they following the same time table as DEFCON/Black Hat (July/Aug in Las Vegas) and the Federal DEFCON was in DC at the end of Sept. then I would assume it will be next year in Sept in DC.
	1115	re 1113: thanks, there's a Microsoft Black Hat in Feb
	1120	re 1115 I know the Federal Black Hat/DEFCON is run by the Las Vegas Black Hat/DEFCON, is the Microsoft Black Hat run by them also?
	1124	re 1120: its the same group, their focus will be securing Microsoft
1079		do we have key performance parameters (KPP'S) id for wireless networks ?
1084		counterpane offers a very good automated monitoring service for civilian companies
1090		make the suggestions and find out
1092		The results of this event will be made available to many people, including policy makers. The results will also probably be provided to people like Dr. Jost and his staff at OAS NII.
1101		yes, towards the ability to say that wireless LANS are needed/wanted, not to make policy
1103		didn't cna do a biz case analysis on wireless lans a few years ago (or was it fo lans) ?
1106		Need to define how this meets CNO goal of a leaner meaner Navy,
1108		2 weeks
1114		For every reel of cable you do not need to take ashore or load on to an MPF ship you can take that much more ordnance or other support gear.
1117		re 1907: We will follow policy from DOD and SECNAV and we will implement solutions approved by CFFC and NETWARCOM. But they will all be based on accreditation from PMW-161. It's that simple.....But you can do all of the above without the information.

## Appendix H, GroupWare Comments

1117		re 1907: We will follow policy from DOD and SECNAV and we will implement solutions approved by CFFC and NETWARCOM. But they will all be based on accreditation from PMW-161. It's that simple.....But you can do all of the above without the information.
1118		SANS is also doing some custom meetings in DC. can't remember the schedule though
1119		for those interested black hat and DEFCON info can be found at blackhat.org and defcon.org
1121		Wireless saves on the logistical platform, Copper, fiber or other cabling, weight, less fuel, time..etc...
	1129	re 1121: Okay, so here's the dumb question. How much wire or cabling is required to install a wireless network as opposed to a wired network that services the same number of customers?
	1139	re 1129: wireless is only going to save you the last 100 feet at best (very few shipboard spaces are larger than that).... agreed, the last 100 feet to each computer but it's still going to require a lot of cabling between the premise router and the access point
	1155	re#1129,1139,1143, considering the GIG and the IP initiative, converge all your services into your wireless, (possible IP capable), your desktop or PDA now replaces your common phone desk, perhaps your desktop computer, your huge VTC into one IP wireless device...do you still save on wire/cable?
1123		RE Policy discussion. I do not see the CDR from the DON CIO office here today, but this forum should take it for action to get a copy of the SECNAV policy that DON CIO has drafted and he briefed about on Monday for review and formal comment. SECNAV is going to issue this policy in response to the DOD 8100.bb policy. So we as this COI for wireless should make sure the Navy policy says what we need it to say. Concur ?
	1133	re: 1123 - The SECNAV policy is being held until 8100.bb is released. Part of the intent is to ensure harmonization.
	1135	re 1123-wanda put on website
	1141	re 1135: Wanda, I'm planning to add a discussion forum for this sort of thing in the NNWC IA N64 community in NKO (Tim)
	1180	RE 1135: Thank you.
1125		Is anyone from OPNAV here?
	1134	re 1125 and other comments: this meeting is being used as a baseline. we are gathered here to see where we stand wrt to policy, security, etc. This is step one of many steps and in my opinion a great beginning!
	1136	re 1134: agreed!
1126		not today
1127		could you get closer to the microphones please...
1128		Speaking of OPNAV and policy, has everyone seen the OPNAV message on implementing GIG-ES?
1130		Another worth while show is Consumer Electronics in Jan. Any new gizmo, gadget, etc is at this show and is held in Jan in Las Vegas

## Appendix H, GroupWare Comments

1131		no, DTG please
1132		"ease and convenience is translated into: Process refinement and efficiencies and Manpower optimization!
1138		How will the DOD RFID policy affect our WLAN ?
	1147	re 1138: good question. As of Jan 05 all DOD suppliers are mandated to have passive RFID tags at the pallet/case level and at the UID item level.
1140		actually I (LCDR Franklin) am here from OPNAV N6F. I have been a silent bug on the wall thus far
	1145	re: 1140 Have you had a chance to talk with N41 folks i.e.; CDR Steve McDonald about impact of DoD RFID Policy and Smart Stores?
	1146	re: 1140. LCDR Franklin, where are you sitting?
1142		I have been noting what I feel are the major issues of the conference (policy guidance, standardization, over application of security, and others). Will take the issues back to my bosses (RADM Zelibor and CAPT Zellman) and brief them on the conference highlights
1143		Cable vs. wire is not a one to one relationship. Can have many more wire drops, more bandwidth, throughput.
1144		Are there other points of interest that any of you think I should report back to OPNAV
1149		What is OPNAV's position on funding for this effort
1150		Funny you should ask that...We recently went through our POM gyrations, however off the top of my head, I don't recall specific set asides to support wireless infrastructure. At present, we are more focused on the security implications and I do know we are focusing IA resources towards the security problem. OPNAV and SECNAV view wireless as technology that we have little choice but to embrace (witness our support for SecNet 11) and feel wireless networks are coming on both the unclas and clas sides in the future. Finally, while NMCI is not initially geared to providing a wireless solution/architecture, the door is open for the contractor to support this requirement in the future. IT21 and BLII will probably provide similar services at some point
1151		Any resources to support the testing of security requirements onboard a ship?
1152		(Fm LCDR Franklin) One addendum...wireless technology is great, but in the near term wired networks will predominate. For now wireless will be limited to areas where there is a validated requirement that can't be filled by a wired solution. There will come a "tipping point" at which the choice between wireless/wired solutions will be a wash in terms of cost, security, administration and efficiency. Of course the question is when that tipping point will be.
	1158	re 1152 - when CFFC comes out with the requirement message, will OPNAV provide funds?
	1161	re 1158 - does this mean we are going to see a message from CNNWC and CFFC validating the "Wireless Requirement" to be forwarded to OPNAV for funding? Is the right place going to be to add it to the ISNS ORD?

## Appendix H, GroupWare Comments

	1164	re: 1158 What I heard Monday that there was that a CFFC message in generation. Don't know the POC so not sure what it will say
	1166	re 1164: Maybe we can ask CDR. Oster...
	1168	rev 1161- you may want to talk with N41 who is working up PR06 estimates for meeting DOD RFID Policy. My personal opinion is that it is not a realistic estimate for doing an entire ship but just one functional area.
	1177	re 1152: will need to check, but don't expect an influx of funds.
1153		We are using the CORONADO and MASON to extrapolate and validate assumptions for now. Small scale experiments are being funded and research is being conducted in places like NPG but these are mainly interesting science projects at the moment. As NETWARCOM grows into a full fledged service N6 they will funnel requirements in a more orderly form to SPAWAR to work the technical issues.
	1160	re: 1153 I would like to discuss our Smart Stores effort which we are working with NSWCCD-Phila. Our working hypothesis is that fully implemented RFID on CVN would reduce the manpower requirement for strike up strike down by approx 65% or more. This is based on a workflow study done by the MH folks and identified where automatic identification technology (AIT) could be used. George Ganak
	1162	re 1160: That is similar to what we are doing on T-AKE. We have been working with Georges AIT team. Larry Urban MSC.
	1163	re 1160: Has this information been sent CNNWC or CFFC to provide the information they need to validate this requirement?
	1165	Re # 1160 RFID is also looked at as an enabler for AWIMS (Aviation Weapon Information Management System)
	1228	Re #1165: who is the PM, or acquisition manager for AWIMS ???
	1232	Re#1228 Mark Husni at NAWC Lakehurst is a good poc to connect with re AWIMS
	1239	RE#1232: THANKS.
1156		lets not forget that submarines are being fitted with wireless LANs and a plethora of data will be available for whomever needs/wants to gather it for reference. However, this is based on WHEN it is installed.

## Roadmapping

MainC mt#	Ref: Cmt #	Comment
1157		Dave Bartlett Begins Roadmap Discussion 1305 Wednesday
1159		The Learning Trust 1310 Wednesday
1167		Yes, good idea



## Appendix H, GroupWare Comments

1169		<p>3 technologies/products have had serious consideration for NAVY testing ... and there are also 3 standards 802.11 b / g &amp; a &gt;&gt;</p> <p>1. SECNET 11 - is 802.11b and restricted to 'B' based on timing and encryption &gt;&gt;&gt; 3 channels available&gt;&gt; most appropriate use is command spaces / SIPRNET</p> <p>2. 3Te systems is 802.11 b or g &gt;&gt; 3 usable channels available &amp; 3X the thru put .. this is focused on mostly HM&amp;E / ICAS applications (NIPR) - these APs are probably not near or co-located with the SIPR sites - so may not have any conflicts or overlap.</p> <p>3. 802.11a systems - is a different frequency (5.9 GHz) with 11 channels available and up to 54 MBPS thru put - these would not interfere with the 802.11b/g &gt;&gt; this system could be used for the admin/pers/training &amp; general staffing NIPR.</p> <p>We don't necessarily need to specify one over the other - or use all three - but if we broadly scope functionality on 'best use' of each of these capabilities - it might be able to optimize the test and evaluation of all of the standards.</p>
	1170	re #1169: can we assume that 802.11a works the same as 802.11b/g especially in a shipboard environment? How much difference in performance and/or interference do we expect between 2.4 and 5 Ghz?
	1171	re 1170 - Good question. I know of no shipboard tests of 802.11a. I would expect different performance characteristics. I think we would need significantly more APs compared to .11b/g to get same coverage.
	1172	#1170 - current commercial white papers showing a vs. b capabilities have the same signal strength & % throughput from 30-300 feet - the "a" then drops off significantly. Shipboard environments has shown to channelize the signal very well for & aft (see notes from much early)... for the admin piece/NIPR this would provide the local/workcenter applications.
	1173	re 1171 I've noticed the market is not doing to well with 802.11a for its lack of interoperability with 802.11.b/g. I fear it may drop out similar to how Lucent did not do too well with their WLAN products for they designed it to FHSS vs. DSSS.
	1174	re 1173: You will start to see 802.11a/b/g routers coming soon in mass to the commercial sector.
	1175	re 1172: The problem is that I believe we have a couple of systems that run at 5Mhz so you may run into some EMI issues. Don't ask me which ones because I have to pull up a brief from last year. This is why all wireless technologies are mandated to go through EMI/EMC testing with the RF suites that are also going to be utilized on that specific platform.

## Appendix H, GroupWare Comments

	1182	re 1172 to add to the quagmire, RFID tags run the spectrum from 13.5mhz all the way up to 5 Ghz and approx 13 flavors in between. Will there be defined frequencies that will be permitted into the WLAN? Or should the WLAN COI be bringing the RFID to this forum? RFID is being driven from the J4 (logistics) arena. And in this case RFID covers both active (batteries needed) and passive (no batteries). There are some newer hybrid tags which can be turned on or off via a "signal". Not sure what freq these run at yet.
	1183	RE 1170: excellent question. and I would add that taking into account the shipboard electromagnetic environment when assessing the differences between 2.4 GHz and 5.8 GHz is also critical. For example, the DDG/CG community has a significantly different EME (Electromagnetic Environment) with their SPY-1 system vice a carrier that does not.
1176		The 802.11a with the different frequency and multiple channel options actually provides a much better military solution if you are worried about EMCOM.. the signal strength drop-off becomes a built-in security feature. since A & B frequencies can operate in the same space without conflict - it provides significant increase in BW capabilities.
1178		802.11a at 5.8 ghz is again in the "unregulated" commercial frequency range - and by definition - should NOT have any EMI conflicts with MIL frequencies.
1179		Mark Theroff Roadmap 1330 Wednesday
1181		A thorough, widely supported roadmap can be a key tool in identifying and raising resources for projects.
1184		I think we do want to bring RFID into this forum. We have not decided what the format will be for future Summits but I think going over general status and then focusing on one or two application categories would be a good format. Maybe RFID will a technology focus for the next summit.
1185		How long did it take to complete the survey?
	1204	re 1185 It took me (PM) approximately 2 1/2 hours. It could have taken longer if I had gotten more detailed.
	1205	re 1204: I'm sure you have that much time to spend on a survey.
1186		30 minutes and 60 minutes on a ship
	1187	re 1186: That's a bit of time.
1188		was survey done via NMIC or otherwise ?
	1189	re: 1188 oops NMCI
1190		Looks web-enabled...I'd be surprised if it worked well from an NMCI seat.
1191		didn't work on my NMCI, but did on my legacy
	1194	re 1191: I was wondering what people used those legacy systems for.
	1195	re #1194: I still had a legacy laptop that was not removed by NMCI
	1197	re 1195: Did you put a trouble call into NMCI for access to the site?
	1198	re 1195: they'll come for it or you can buy it.....
1192		Thought so
1193		The survey was done via the web.

## Appendix H, GroupWare Comments

1196		If it was a web-enabled survey, why wouldn't it work from an NMCI seat?
	1199	re 1196: Not all web-sites work on an NMCI seat.
1200		Funny, I don't know why, it just didn't
1201		Was it delivered from a .mil domain?
	1203	re 1201: It shouldn't have to be a .MIL domain.
1202		no
1206		Do you have time to be here? If so, what's a couple of hours for a survey?
	1207	re 1206 - a lot when you don't have it
	1215	re: 1206: The time is worth it if everyone can begin collaborating. Two hours answering a survey may save someone else weeks by leveraging off what you learned. This is a key element in forming the wireless community of interest.
1208		This Road Mapping tool looks like an overrated POA&M
	1209	re 1208: I'm sure it is a pretty cheap tool....
	1213	re: 1208: Agreed.
	1222	re 1208-project on steroids, but useful when working in this virtual community of interest/experts on an issue that is across several organizations. A great display/graphic tool and a communication method.
1210		What is POA&M?
1211		Plan of action and milestone
1212		Thanks.
1216		Precisely
1217		WIFM ?
	1218	re1217: ??
	1221	re 1217: I know what WTF stand for but not WIFM.
	1224	re 1217: You may save weeks from 2 hrs that someone else put into a survey. And having a roadmap helps the whole community raise resources.
1219		what's in it for me....
1220		I can see a benefit for a sort of trend analysis for programs, but is this going to show a critical path?
1223		Does this provide a technology readiness level assessment?
1225		hopefully we can enter documents for other folks to use - SSAA's, test results, etc.
	1226	re: 1225: Yes, you can do that.
1227		links are the best way after docs are scanned and submitted as mentioned
	1229	re 1227: As long as the links stay current...the actual docs uploaded may be the best solution.
	1230	re 1229: Agreed. That can be done.
1231		The question is, if we want to collaborate and put together a big picture of what is going on and where are we going with wireless networks in the Navy, how are we going to accomplish that? This roadmapping approach is one possible method. It is by no means the only approach. If others have better suggestions, make them.
	1234	RE: 1231- How about setting up a community on NKO?

## Appendix H, GroupWare Comments

	1237	re 1231: The roadmapping tool is SQL based, which makes it easy to import data from other orgs that roadmap with this tool, such as Motorola. If this becomes a widely adopted standard, it will make it very easy to share and coordinate activities between ONR, the Wireless COI, industry, universities, etc.
1233		Understand what you're saying, but how does this tool relate to a road map?
1235		we should be more concerned with the data, not how it looks
	1241	re 1235: Ease of visualization is just as important as having the data.
1236		what does ntira stand for and who owns ?
1238		We will be setting up a community on NKO. That is another method for collaboration.
1240		What guidance can I provide weapon system programs that are currently/planning to field wireless into the IT-21/NTCSS and/or soon to be NMCI environment for life cycle support - will this group's planning include a handoff mechanism for sustainment/refresh??
1242		How would one update documents in the Road Mapping tool?
1243		Elvis is about to leave the bldg. If you have specific questions concerns, I may be contacted at:  Tel: 703 604 7855

## Summary Discussion

MainC mt#	Ref: Cmt #	Comment
1245		Final Words 1440 Wednesday

## APPENDIX I: REFERENCES

1. IEEE Wireless Standards, <http://standards.ieee.org/wireless>
2. DoD Information Technology Security Certification and Accreditation Process (DITSCAP), <http://iase.disa.mil/ditscap>
3. National Information Assurance Partnership Website, <http://niap.nist.gov>
4. Pentagon Area Common Information Technology Wireless Security Policy, Office of the Secretary of Defense, September 25, 2002
5. Department of Defense Directive 8100.bb, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid, Draft.
6. Harris Corporation SecNET 11 Secure Wireless Local Area Network, <http://www.govcomm.harris.com/secure-comm>
7. Common Criteria for IT Security Evaluation, <http://csrc.nist.gov/cc>
8. Wireless Task Force Report, Wireless Security by National Security Telecommunications Advisory Committee, January 2003.
9. Wireless LAN 802.11b Security FAQ, [http://www.iss.net/wireless/WLAN\\_FAQ.php](http://www.iss.net/wireless/WLAN_FAQ.php)
10. Federal Information Processing Standards Publication FIPS PUB 140-2 May 25, 2001 updated December 3, 2002 Security Requirement for Cryptographic Modules, <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
11. 3e Technologies International Website, <http://www.3eti.com>
12. Program Executive Office Ships, <http://peos.crane.navy.mil>
13. Naval Network Warfare Command (NETWARCOM), <http://www.netwarcom.navy.mil>

## Appendix I, References

Intentionally Left Blank